

MFN 07-515

Enclosure 2

**GEH Nuclear Energy, “ESBWR I&C TRICON (SSLC/ESF)
Platform Application,” NEDO-33388P, Revision 0,
September 2007 – Non-proprietary Version**

NEDO-33388
Revision 0
Class I
September 2007

Licensing Topical Report

**ESBWR I&C
TRICON (SSLC/ESF)
PLATFORM APPLICATION**

Ira Poppel

Copyright 2007 GE-Hitachi Nuclear Energy

NONPROPRIETARY INFORMATION NOTICE

This is a nonproprietary version of the document NEDE-33388P, Revision 0, where the proprietary information of NEDE-33388P, Revision 0 has been removed. The portions of NEDE-33388P, Revision 0 that have been removed are indicated by double square open and closed brackets as shown here [[]]. Figures and large equation objects of NEDE-33388P, Revision 0 that have been removed are also identified with double square brackets before and after where the object was to preserve the relative spacing of NEDE-33388P, Revision 0.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The information contained in this document is furnished for the purpose of obtaining NRC approval for the use of a TRICON Programmable Logic Controller for SSLC/ESF application for the ESBWR. The only undertakings of GEH respecting information in this document are contained in the contracts between GEH and the participating utilities in effect at the time this report is issued, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table Of Contents

1.0	INTRODUCTION.....	1
1.1	ARCHITECTURE OVERVIEW	2
1.2	SUMMARY AND CONCLUSIONS	3
1.2.1	<i>Meeting Probabilistic Safety-Related Goals.....</i>	<i>3</i>
1.2.2	<i>Compliance with NUREG-0493 and NUREG/CR-6303.....</i>	<i>6</i>
1.2.3	<i>Compliance with Safety System Design Requirements</i>	<i>6</i>
2.0	DESIGN BASES.....	7
2.1	EMERGENCY CORE COOLING SYSTEM DESCRIPTION	7
2.1.1	<i>PASSIVE CONTAINMENT COOLING SYSTEM.....</i>	<i>7</i>
2.1.2	<i>ISOLATION CONDENSER SYSTEM.....</i>	<i>7</i>
2.1.3	<i>GRAVITY DRIVEN COOLING SYSTEM.....</i>	<i>8</i>
2.1.4	<i>AUTOMATIC DEPRESSURIZATION SYSTEM.....</i>	<i>8</i>
2.1.5	<i>STANDBY LIQUID CONTROL SYSTEM.....</i>	<i>8</i>
2.2	SSLC/ESF SUPPORT AND CONTROL FUNCTIONS	8
2.2.1	<i>Control Room Habitability.....</i>	<i>9</i>
2.2.2	<i>Containment Monitoring System</i>	<i>9</i>
2.2.3	<i>Post Accident Monitoring System.....</i>	<i>11</i>
2.2.4	<i>Leak Detection and Isolation System (LD&IS).....</i>	<i>11</i>
2.3	SSLC/ESF REQUIRED CAPABILITIES.....	11
2.3.1	<i>Safety-Related Displays/Control.....</i>	<i>11</i>
2.3.2	<i>Alarms.....</i>	<i>11</i>
2.3.3	<i>Communications</i>	<i>11</i>
2.3.4	<i>Data Acquisition.....</i>	<i>12</i>
2.3.5	<i>Actuator Outputs.....</i>	<i>12</i>
2.3.6	<i>Power.....</i>	<i>12</i>
3.0	TRICON CAPABILITIES	13
3.1	DESCRIPTION	13
3.2	EXPANSION/REMOTE DATA ACQUISITION	15
3.3	DATA ACQUISITION	15
3.4	COMMUNICATION	18
4.0	APPLICATION.....	19
4.1	COMMON Q-DCIS APPLICATION AND OVERVIEW	19
4.1.1	<i>General Data and Electrical Isolation</i>	<i>19</i>
4.1.2	<i>General Logic Configuration</i>	<i>20</i>
4.1.3	<i>Diversity</i>	<i>23</i>
4.1.4	<i>Power.....</i>	<i>28</i>
4.1.5	<i>Separation.....</i>	<i>28</i>
4.2	SPECIFIC SSLC/ESF APPLICATION	28
4.2.1	<i>TRICON Configuration</i>	<i>28</i>
4.2.2	<i>Location.....</i>	<i>29</i>
4.2.3	<i>Per Division SSLC/ESF arrangement.....</i>	<i>29</i>
4.2.4	<i>Standard Data Acquisition</i>	<i>36</i>
4.2.5	<i>SSLC/ESF Discrete Outputs</i>	<i>37</i>
4.2.6	<i>TRICON Communications</i>	<i>42</i>
4.2.7	<i>TRICON VDUs</i>	<i>49</i>
4.2.8	<i>TRICON Security.....</i>	<i>50</i>

5.0	NRC CERTIFICATION – GE RESPONSE TO OPEN ITEMS	59
5.1	ITEM #1: QUALIFICATION FOR TEMPERATURE AND HUMIDITY CONDITIONS.	59
5.2	ITEM #2: QUALIFICATION FOR RADIATION EXPOSURE LEVELS.	59
5.3	ITEM #3: QUALIFICATION FOR SEISMIC LEVELS.	59
5.4	ITEM #4: QUALIFICATION FOR EMI/RFI: CONDUCTED OR RADIATED EMISSIONS.	60
5.5	ITEM #5: SURGE WITHSTAND CAPABILITY.....	60
5.6	ITEM #6: ELECTROSTATIC DISCHARGE (ESD) WITHSTAND CAPABILITY.....	60
5.7	ITEM #7: SAFETY-RELATED TO NONSAFETY-RELATED ISOLATION FROM CREDIBLE VOLTAGES.	61
5.8	ITEM #8: SOFTWARE INSTALLATION PLAN DEVELOPMENT.....	61
5.9	ITEM #9: SOFTWARE MAINTENANCE PLAN DEVELOPMENT.	61
5.10	ITEM #10: SOFTWARE OPERATIONS PLAN DEVELOPMENT.....	61
5.11	ITEM #11: SOFTWARE SAFETY PLAN DEVELOPMENT.....	62
5.12	ITEM #12: SOFTWARE VERIFICATION AND VALIDATION.	62
5.13	ITEM #13: IMPACT OF TRISTATION 1131 USE OF TRICON PLC OPERABILITY.	62
5.14	ITEM #14: PLANT SPECIFIC APPLICATION PROGRAM.	62
5.15	ITEM #15: COMPONENT AGING ANALYSIS.....	63
5.16	ITEM #16: RESPONSE TIME CHARACTERISTICS.....	63
5.17	ITEM #17: DIVERSITY AND DEFENSE-IN DEPTH (D3).....	63
5.18	ITEM #18: QUALIFICATION SUMMARY REPORT “APPLICATIONS GUIDE” RECOMMENDATIONS.	64
6.0	REFERENCES.....	65

List of Tables

TABLE 4-1 EXAMPLE ASSIGNMENT OF DPV SQUIB VALVE IGNITORS TO SSLC/ESF AND DPS.....	22
TABLE 4-2 SSLC/ESF PLANT LOCATIONS.....	31

List of Figures

FIGURE 1-1 ESBWR DCIS ARCHITECTURE BLOCK DIAGRAM.....	4
FIGURE 1-2 ESBWR DCIS ARCHITECTURE SCHEMATIC.....	5
FIGURE 2-1 ESBWR ECCS CONFIGURATION.....	10
FIGURE 3-1 TRICON TMR PROCESSING CONFIGURATION.....	14
FIGURE 3-2 TRICON MAIN CHASSIS.....	16
FIGURE 3-3 TRICON EXPANSION CAPABILITY.....	17
FIGURE 4-1 ESBWR SSLC/ESF LOGIC ARCHITECTURE.....	21
FIGURE 4-2 HARDWARE/SOFTWARE (PLATFORM) DIVERSITY.....	24
FIGURE 4-3 ESBWR SYSTEMS DIVERSITY.....	25
FIGURE 4-4 ESBWR Q-DCIS POWER.....	26
FIGURE 4-5 ESBWR DCIS AND POWER SEPARATION.....	27
FIGURE 4-6 SSLC/ESF (TRICON) CONFIGURATION.....	30
FIGURE 4-7 DIVISION 1 SSLC/ESF (TRICON) CONFIGURATION.....	32
FIGURE 4-8 DIVISION 2 SSLC/ESF (TRICON) CONFIGURATION.....	33
FIGURE 4-9 DIVISION 3 SSLC/ESF (TRICON) CONFIGURATION.....	34
FIGURE 4-10 DIVISION 4 SSLC/ESF (TRICON) CONFIGURATION.....	35
FIGURE 4-11 TRICON CABINET C63-PL-X101 DETAIL.....	39
FIGURE 4-12 TRICON CABINET C63-PL-X102 DETAIL.....	40
FIGURE 4-13 DIVISION 1 TRICON COMMUNICATIONS.....	44
FIGURE 4-14 DIVISION 2 TRICON COMMUNICATIONS.....	45
FIGURE 4-15 DIVISION 3 TRICON COMMUNICATIONS.....	46
FIGURE 4-16 DIVISION 4 TRICON COMMUNICATIONS.....	47
FIGURE 4-17 TRICON COMMUNICATIONS MODULE.....	52
FIGURE 4-18 TRICON COMMUNICATIONS SECURITY.....	54
FIGURE 4-19 TRICON/VDU COMMUNICATIONS.....	56
FIGURE 4-20 TRICON MESSAGE STRUCTURE.....	57

LIST OF ACRONYMS AND ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
AC	Alternating Current
ADS	Automatic Depressurization System
AFIP	Automatic Fixed In-Core Probe
ALWR	Advanced Light Water Reactor
AOO	Anticipated Operational Occurrence
APRM	Average Power Range Monitor
ARI	Automatic Rod Insertion
ASME	American Society of Mechanical Engineers
ATLM	Automatic Thermal Limit Monitor
ATWS	Anticipated Transients without SCRAM
BiMAC	Basemat-internal Melt Arrest Coolability
BOP	Balance of Plant
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CB	Control Building
CCF	Common Cause Failure
CIM	Communication Interface Module
CMF	Common-Mode Failure
COL	Combined Operating License
CRD	Control Rod Drive
DAS	Data Acquisition System
DATALINK	A communication path between two systems – almost always by fiber-optic cable
DC	Direct Current
DCD	Design Control Document
DCIS	Distributed Control and Information System
DI	Digital Input
DPS	Diverse Protection System
DPV	Depressurization Valve
DS	Deluge System
ECCS	Emergency Core Cooling System
EQV	Equalizing Valve
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference

EOF	Emergency Offsite Facility
EPA	Electric Protection Assembly
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature (ESF) Actuation System
ETP	External Termination Panel
FAPCS	Fuel and Auxiliary Pools Cooling System
FB	Fuel Building
FMCRD	Fine Motion Control Rod Drive
FOAKE	First-of-a-Kind Engineering
FW	Feedwater
FWCS	Feedwater Control System
GATEWAY	A device representing a “translator” between two datalinked systems
GDC	General Design Criterion
GDCS	Gravity Driven Cooling System
GDS	Gated Diode Switch
HCU	Hydraulic Control Unit
HFE	Human Factors Engineering
HMI	Human-Machine Interface
HP	High Pressure
HSI	Human-System Interface
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation & Control
ICS	Isolation Condenser System
IEEE	Institute of Electrical and Electronics Engineers
INOP	Inoperable
kV	Kilovolt (1000 volts)
LD&IS	Leak Detection and Isolation System
LFCV	Low Flow Control Valve
LOCA	Loss of Coolant Accident
LPRM	Local Power Range Monitor
Mark*VIe	General Electric Dual or Triply redundant controller
MCC	Main Control Console
MCR	Main Control Room
MOV	Motor Operated Valve
MP	Main (TRICON) Processor

MRBM	Multi-Channel Rod Block Monitor
MSIV	Main Steam Isolation Valve
N-DCIS	Nonsafety-related Distributed Control and Information System
NDL	Nuclear Data Link
NI	Nuclear Island
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control
PAS	Plant Automation System
PCCS	Passive Containment Cooling System
PCF	Plant Computer Function(s) (Sub-system of N-DCIS)
PIP	Plant Investment Protection
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PS	Power Supply
PSWS	Plant Service Water System
Q-DCIS	Safety-related Distributed Control and Information System
RB	Reactor Building
RBM	Rod Block Monitor
RC&IS	Rod Control and Information System
RCCW	Reactor Closed Cooling Water System
RCS	Reactor Coolant System
RG	Regulatory Guide
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown System
RTIF	Reactor Trip and Isolation Function
RMU	Remote Multiplexing Unit
RWCU/SDC	Reactor Water Cleanup System/Shutdown Cooling System
RWM	Rod Worth Minimizer
SB&PC	Steam Bypass and Pressure Control
SBO	Station Blackout
SBWR	Simplified Boiling Water Reactor
SCRRI	Selected Control Rod Run-In

SDO	Supervised Digital Output
SLCS	Standby Liquid Control System
SPDS	Safety Parameter Display System (Sub-system of N-DCIS)
SRI	Select Rod Insert
SRNM	Source Range Neutron Monitor
SRV	Safety-Relief Valve
SSC	Shift Supervisor's Console
SSLC	Safety System Logic and Control
TBV	Turbine Bypass Valve
TC	Thermocouple
TCCW	Turbine Component Cooling Water
TCM	TRICON Communication Module
TGCS	Turbine Generator Control System
TMI	Three Mile Island
TMR	Triple Modular Redundant
TSC	Technical Support Center
UDP/IP	User Datagram Procol/Internet Protocol
VDU	Video Display Unit (in this document the VDUs are assumed to be touch screen but further HFE analysis may dictate other operator pointing devices)
WDP	Wide Display Panel

1.0 INTRODUCTION

The ESBWR is one of the first next generation of light water reactors to replace older technology hard wiring, meters and recorders, relays, and single channel analog instrumentation with a modern distributed control and information system (DCIS) design. Since the Simplified Boiling Water Reactor (SBWR) and Advanced Boiling Water Reactor (ABWR) were originally designed there have been dramatic changes and improvements in power plant DCIS, and there has been a slow but continuous introduction of retrofit safety-related and nonsafety-related digital control systems into operating nuclear power plants. The control systems concepts have been further improved as part of the U.S. certification and First-of-a-Kind Engineering program (FOAKE) of the ABWR that incorporated industry guidance and requirements from the Advanced Light Water Reactor (ALWR) Utility Requirements Document together with experience gained from the delivery of the ABWR DCIS in Japan and, most recently, Taiwan (where U.S. standards were closely followed). The ESBWR use of DCIS includes both safety-related (Q-DCIS) and nonsafety-related (N-DCIS) control and information system functions.

The Q-DCIS includes both the Reactor Protection System/Neutron Monitoring System (RPS/NMS) and the Safety System Logic and Control/Engineered Safety Feature (SSLC/ESF) systems; this report documents the application of the TRICON as the SSLC/ESF hardware/software platform. The N-DCIS indirectly contributes to plant safety because many power generation single failures have been eliminated by using at least dual redundant nonsafety-related control design.

Additional DCIS design features have been incorporated because of the ESBWR passive safety-related systems and new regulatory requirements that must also be considered in the overall DCIS design:

- Probabilistic Risk Assessment (PRA) methods are used to consider the role of both safety-related and nonsafety-related equipment in the prevention and mitigation of transients and faults. This consideration is reflected in the overall design of the DCIS and mechanical systems.
- The inclusion of N-2 as a Q-DCIS design basis; N-2 refers to the ability of the ESBWR DCIS to meet all safety-related functions with any two of four random divisions out of service.
- The importance of preventing inadvertent action of some ECCS functions.
- The nonsafety-related Diverse Protection System (DPS) provides a subset of reactor trip, isolation and ESF actuations diverse from the Q-DCIS. The DPS is included in the design to reduce the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated Common-Mode Failures (CMFs).

Notwithstanding the presence of the DPS in the ESBWR design (with its assumption of common cause Q-DCIS failure), the Q-DCIS design meets all applicable regulatory requirements and, in general, is robust enough to both reliably initiate and monitor the ECCS and to reliably avoid its inadvertent initiation.

1.1 ARCHITECTURE OVERVIEW

The Q-DCIS includes the Nuclear Measurement Analysis and Control (NUMAC) and TRICON hardware/software platforms; the NUMAC platform provides RPS, NMS, Main Steam Isolation Valve (MSIV) / Leak Detection and Isolation (LD&IS) functions. The ESBWR also includes N-DCIS functions on a hardware/software platform diverse from both NUMAC and SSLC/ESF. The TRICON platform is the SSLC/ESF and provides the ECCS functions; its application for those tasks is the subject of this report.

The DCIS systems are shown in block diagram form in Figure 1-1 and schematically in Figure 1-2; the safety-related Q-DCIS, located in the lower left, is a safety-related I&C system that is included in the ESBWR DCIS architecture to address Design Basis Events outlined and described in Chapter 15 of the ESBWR Design Control Document (DCD) (Reference 1). The Q-DCIS design complies with NEDE-33245P – Software QA Plan (Reference 2) and NEDE-33226P – Software Management Plan (Reference 3) and specifically meets plant licensing requirements by including design features such as:

- Redundancy
- Functional diversity
- Failsafe design (RPS, NMS, and MSIV LD&IS)
- Continuous self-diagnostics
- Periodic surveillance test capability
- Isolation (between safety-related divisions and between safety-related divisions and nonsafety-related components)
- A design verification and validation process

The DPS provides a subset of automatic reactor shutdown and ECCS protection using sensors, processors, and actuators that are diverse from those in Q-DCIS. Specifically the triply redundant processors of DPS make two-out-of-four sensor trip decisions and when two of the inputs to the three processors agree that a trip is required, the reactor is scrammed, isolation valves are closed, or the ECCS is initiated.

The N-DCIS cabinets and components are located in one of two nonsafety-related DCIS rooms; although also nonsafety-related, the DPS control cabinet is located apart from the other N-DCIS cabinets. The four divisional safety-related control systems of the Q-DCIS are physically separated from each other, from the non-safety-related control systems of the N-DCIS, and from the DPS. The two trains of the nonsafety-related plant investment protection (PIP) system controllers are physically separated from each other and from the Q-DCIS and the DPS. The DPS is physically separated from the two PIP trains and the Q-DCIS.

All communication to/from the field Remote Multiplexing Units (RMUs) is by fiber optic cable (fiber), and all communication from the DCIS rooms to the main control room (MCR) safety-related and nonsafety-related Video Display Units (VDUs) are via fiber. The few hard-wired exceptions are for signals like main turbine trip or reactor manual SCRAM signals. These MCR considerations are important because the communications protocol is such that a compromised fiber will not cause erroneous operation nor affect the continued operation of all automatic safety-related or nonsafety-related systems. This is also supported by the fact that touch screen operation of the VDUs requires several

operator actions whose resulting communication is unlikely to be replicated by communications loss or damage; similarly the DCIS represents a distributed network whose nodal addresses are equally unlikely to be replicated by fiber loss.

The operator interface functions of the DCIS define the arrangement of the MCR, the layout of the DCIS equipment on the main bench boards (and remote system shutdown (RSS) panels), and dictate the design process for the layout and content of operating and safety-related displays, alarms, controls, and procedures for the Human-System Interface (HSI). The HSI functions, developed under the formal Human Factors Engineering (HFE) plans, are defined in the appropriate instrumentation and control (I&C) system sections (Reference 1).

The MCR has eight divisional VDUs (two per division) from which safety-related systems can be both monitored and controlled. The safety-related VDUs, although using touch screen technology and having the same operator "look and feel," use technology diverse from that of the nonsafety-related VDUs. The safety-related VDUs are completely isolated from the N-DCIS.

1.2 SUMMARY AND CONCLUSIONS

1.2.1 Meeting Probabilistic Safety-Related Goals

The analysis of protection against various ESBWR transients and accidents, including common-mode failures (CMF) is documented in Chapter 15 of Reference 1 and is conducted in parallel with the development of the Probabilistic Risk Assessment (PRA) (Reference 4). The preliminary conclusion is that the I&C architecture, specifically including Q-DCIS and TRICON is, as calculated by the PRA analysis to date, sufficient to meet probabilistic safety-related goals. As further design detail becomes available and the PRA is updated, the response (including failures) of the DCIS architecture, including common cause failures, will be analyzed.

Figure 1-1 ESBWR DCIS Architecture Block Diagram

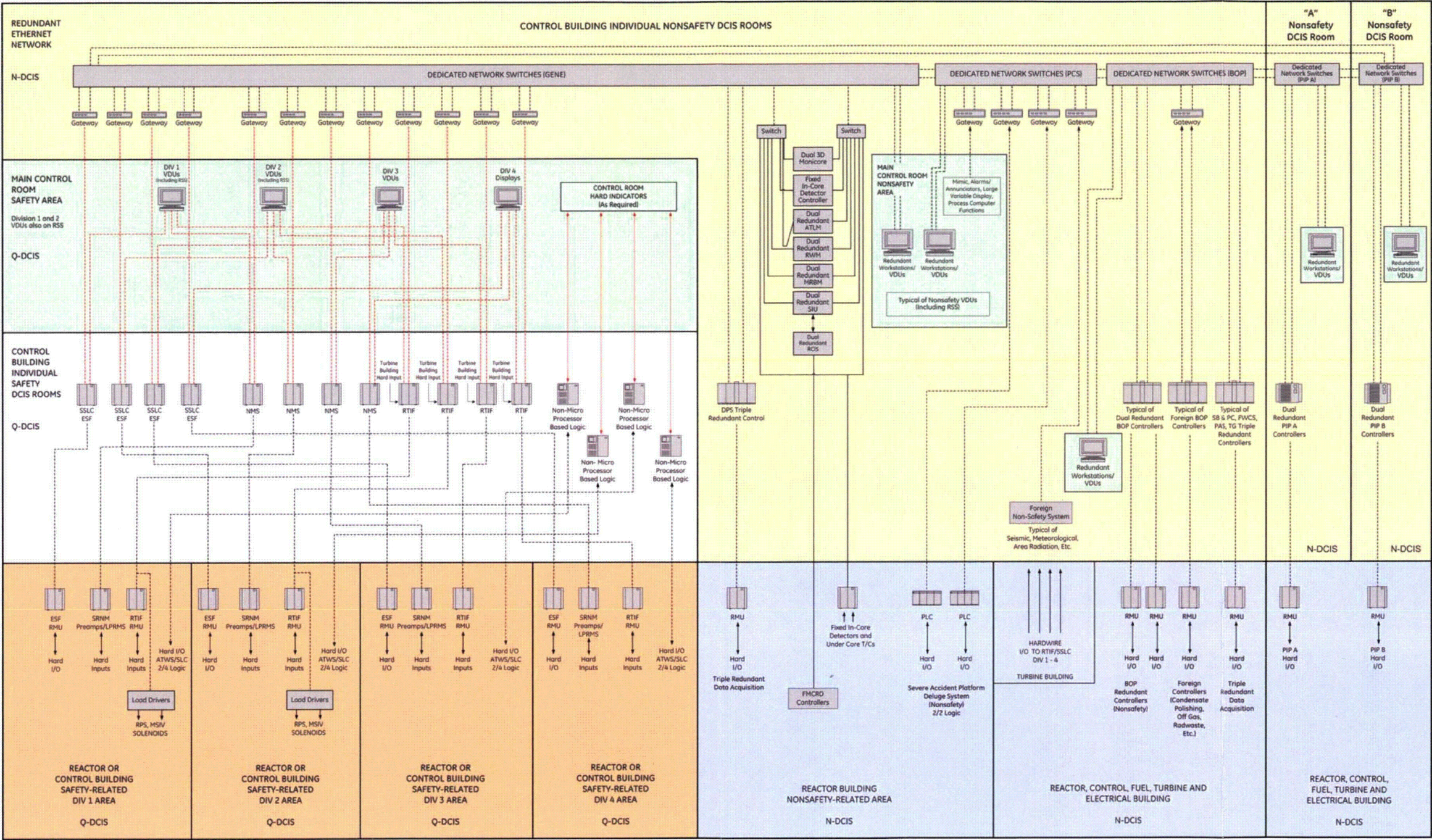
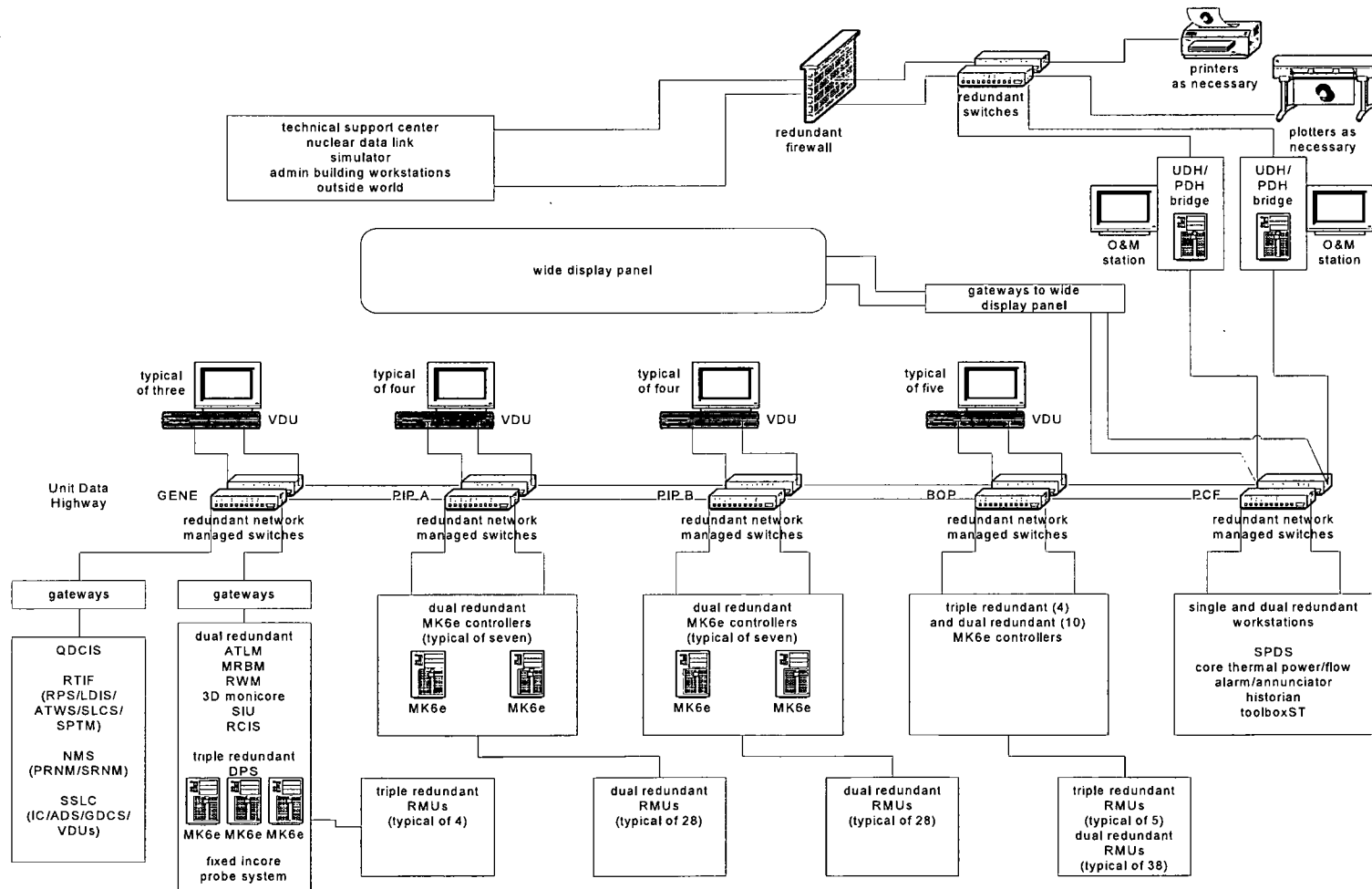


Figure 1-2 ESBWR DCIS Architecture Schematic



1.2.2 Compliance with NUREG-0493 and NUREG/CR-6303

The DCIS architecture meets the expectations of NUREG-0493 (Reference 5), in particular, Section 2, “Technical Discussion” and Section 3.3 “Guidelines,” which contain guidelines, requirements, and recommendations. The DCIS architecture complies with NUREG/CR-6303 (Reference 6), in particular, Section 3 “Guidelines,” which contains guidelines, requirements, and recommendations.

1.2.3 Compliance with Safety System Design Requirements

The DCIS architecture and specifically the TRICON SSLC/ESF application meets the requirements of IEEE 603-1998, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (Reference 7), IEEE 379-2000, “IEEE Standard Application of the Single-failure Criterion to Nuclear Power Generating Station Safety Systems – Description” (Reference 8), R.G. 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems,” May 1973 (Reference 9), and General Design Criterion 24, Separation of Protection and Control Systems (Reference 10).

2.0 DESIGN BASES

2.1 EMERGENCY CORE COOLING SYSTEM DESCRIPTION

The ESBWR is a passive plant meaning that nuclear safety is achieved without using active, safety-related electrical power sources, pumps, motor operated valves or pumped water heat removal. Instead, the ESBWR relies on gravity and natural circulation to implement ECCS functions. Specifically, the ESBWR ECCS includes the:

- Passive Containment Cooling System (PCCS)
- Isolation Condenser System (ICS)
- Gravity Driven Cooling System (GDCS)
- Automatic Depressurization System (ADS)
- Standby Liquid Control System (SLCS)

These systems are shown in Figure 2-1.

2.1.1 PASSIVE CONTAINMENT COOLING SYSTEM

The PCCS consists of six heat exchangers, each located in its own pool of water. Each heat exchanger has a continuously open connection to the drywell such that any steam generated in the drywell (or wetwell) is automatically directed to the top of the heat exchanger. Since the heat exchanger is placed in a pool of cool water, the drywell steam is condensed and drained to the GDCS pools. This is a low pressure system with no valves in either the inlet or discharge to/from the heat exchanger. There are no initiation signals nor operating system logic since operation is completely automatic and passive. The steam side of the heat exchanger is part of the containment pressure boundary.

2.1.2 ISOLATION CONDENSER SYSTEM

The ICS consists of four heat exchangers each located in its own pool of water. Each heat exchanger has normally open isolation valves on the inlet (steam) and discharge (condensed water) but additionally includes normally closed condensate return valves. The heat exchanger inlet is connected to the reactor pressure vessel (RPV) steam lines and the heat exchanger discharge is connected to the RPV. The ICS is initiated by opening the condensate return valves, and because the heat exchanger is placed in a pool of cool water, the reactor steam is condensed and returned to the RPV. This is a high pressure system and has the advantage of being able to cool and depressurize the reactor without losing vessel inventory (as would a relief valve), operates whether or not the RPV is isolated and does not require that the reactor be depressurized. The steam side of the heat exchanger has the same pressure rating as the RPV. All valves in the ICS are solenoid-operated.

For both the PCCS and ICS, the ultimate heat sink is the atmosphere since eventually the steam condensation process will heat up and boil the pool water. Even boiling pool water will still condense the steam released in an accident and the pools are sized to boil for three days without requiring makeup. There are several methods for either cooling the pools or adding post-accident water in the absence of offsite power and the nonsafety-related diesel generators.

The heat exchangers are monitored for high steam or condensate return flow and the pool air space is monitored for radiation; conditions exceeding setpoints indicate a leak for which the SSLC/ESF isolates the heat exchanger.

2.1.3 GRAVITY DRIVEN COOLING SYSTEM

The GDACS consists of three pools of water located inside containment; two of these pools have a single discharge line to the RPV and the third pool has two discharge lines to the RPV. All four discharge lines employ both check valves and squib valves that normally provide a leak tight seal. However, when the squib valves are fired, they create a low resistance path from the pools to the RPV. The GDACS also includes lines from the suppression pool to the RPV that include squib valves; most of the suppression pool is located above the top of the reactor core.

The GDACS is initiated by firing the squib valves (GDACS pools first, suppression pool later, should RPV water level continue to fall). If the RPV has been depressurized to containment pressure, water will flow by gravity to the RPV and passively keep the core covered. Because the containment is a closed system whose heat is continuously being removed by the PCCS, the core stays covered indefinitely (as long as the ICS/PCCS pools are kept supplied with water).

Although not part of GDACS/ECCS, the GDACS pools (through separate squib valves) can also supply water to the severe accident under vessel basemat-internal melt arrest coolability (BiMac) deluge system.

2.1.4 AUTOMATIC DEPRESSURIZATION SYSTEM

The GDACS requires that the reactor be depressurized before the water in its pools can flow to the RPV; the ADS performs this depressurization function. ADS comprises 10 (of eighteen) safety-relief valves (SRV) and eight squib-actuated depressurization valves (DPV). The SRVs are mounted on the main steam lines, four of the DPV are mounted on the ICS steam supply lines, and the remaining four DPV on "stub" steam lines from the RPV. The SRVs are discharged to the suppression pool and the DPVs to the drywell (containment) atmosphere.

When a low RPV water level signal is present for a specified time, the ADS sequentially initiates the SRVs, followed by the DPVs; this avoids RPV level swell and possible RPV inventory loss while depressurizing the reactor quickly enough to allow GDACS flow to prevent the core from being uncovered.

2.1.5 STANDBY LIQUID CONTROL SYSTEM

Although primarily a reactivity control system, the SLCS is also initiated as an ECCS function. The system incorporates two pressurized accumulator tanks filled with borated water and initiated by squib valves. The safety-related logic is non-microprocessor based and diverse from both NUMAC and TRICON. The four TRICON SSLC/ESF divisions supply a two out of four low water level SSLC initiation demand signal to each division of ATWS/SLCS logic.

2.2 SSLC/ESF SUPPORT AND CONTROL FUNCTIONS

The SSLC/ESF is not only used to initiate the ECCS but provides other safety-related functions as indicated below.

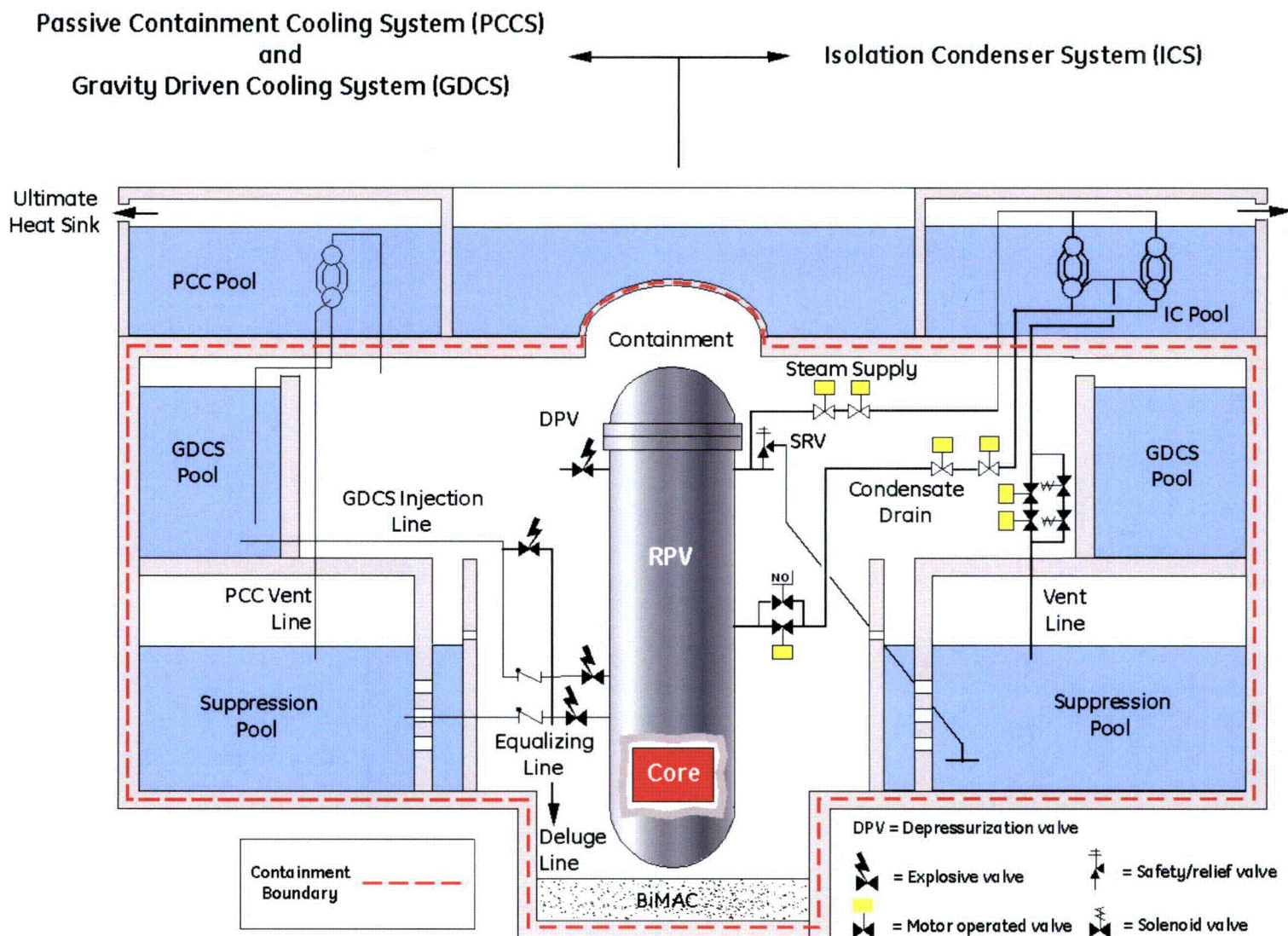
2.2.1 Control Room Habitability

The SSLC/ESF provides the control, monitoring and automatic initiation of the safety-related emergency filtration systems used to promote post accident control room habitability.

2.2.2 Containment Monitoring System

The SSLC/ESF provides the data acquisition, monitoring/display, and alarm management of the necessary safety-related parameters needed to monitor containment liquid levels, atmospheric pressures, and radiation levels.

Figure 2-1 ESBWR ECCS Configuration



2.2.3 Post Accident Monitoring System

The SSLC/ESF provides the data acquisition, monitoring/display, and alarm management of the necessary safety-related parameters needed to support post-accident monitoring as defined by Regulatory Guide 1.97 (Reference 11).

2.2.4 Leak Detection and Isolation System (LD&IS)

The SSLC/ESF provides the logic, data acquisition, control outputs, monitoring/display, alarm management and operator inputs needed to automatically and manually isolate the various (non-MSIV) process lines needed to prevent radiation releases to the public.

2.3 SSLC/ESF REQUIRED CAPABILITIES

In order to support the above functions the SSLC/ESF TRICON platform has specific capabilities that are discussed in the following subsections:

2.3.1 Safety-Related Displays/Control

The SSLC/ESF provides a safety-related capability to allow the operator to monitor and alarm safety-related parameters needed to operate the ECCS and support functions. The displays also provide the operator with the capability to input actions needed to control and initiate these systems.

2.3.2 Alarms

The SSLC/ESF provides a safety-related alarm system that, in the absence of N-DCIS, alerts the operator to abnormal safety-related plant conditions. Included are both process alarms (related to ESBWR plant parameters) and diagnostic alarms that monitor the Q-DCIS hardware and software.

2.3.3 Communications

The SSLC/ESF supports communication between:

- TRICON and TRICON – this represents the division to division communication needed to support the two out of four logic used for ECCS initiation and isolation signals. These communication paths are by fiber and redundant.
- NUMAC and TRICON – this communication stays within a division and is required to allow NUMAC NMS and RPS status and alarms to be displayed on safety-related VDUs. The communication is one way in that safety-related displays are not used to control the NMS or RPS. These communication paths are by fiber and redundant.
- TRICON and N-DCIS – this communication path is used to send safety-related plant data, diagnostics and alarms to the nonsafety-related DCIS for further display, recording and alarming. Each division has its own link to N-DCIS, and the links are both data and electrically isolated. The same link is used to send time-of-day from N-DCIS to SSLC/ESF to be used in time tagging data returned to N-DCIS (for analysis) and for VDU displays. The time-of-day is never used in the safety-related logic, synchronization of divisions or any safety-related function. The link does not allow or support N-DCIS control of any safety-related system and is not used to send NUMAC RPS/NMS

information to N-DCIS (these systems have their own data links). These communication paths are by fiber and redundant.

2.3.4 Data Acquisition

The SSLC/ESF is able to reliably acquire safety-related data from assigned areas of the control building (CB) and reactor building (RB) and direct them to the safety-related processors performing SSLC/ESF functions. The types of signals include:

- 4 – 20 ma process transducer outputs
- Thermocouple outputs
- RTD outputs
- Field contact status
- Voltage changes

2.3.5 Actuator Outputs

The SSLC/ESF is able to reliably actuate solenoids and squib actuators and reliably avoid inadvertent actuation of those devices. Generally SSLC/ESF provides power for the actuated devices.

2.3.6 Power

The SSLC/ESF has redundant internal power supplies, accepts two separate power feeds, and is able to support all safety-related functions with only one power supply or power feed operable. Both power feeds are required to support 72 hours of operation for station blackout (SBO) events.

3.0 TRICON CAPABILITIES

This section describes important features of the TRICON that are used to support ESBWR SSLC/ESF functions.

3.1 DESCRIPTION

The TRICON is a programmable logic controller (PLC) that provides fault tolerance by means of a Triple-Modular Redundant (TMR) architecture; a functional drawing of the TMR architecture is shown in Figure 3-1. TMR integrates three isolated, parallel control systems and extensive diagnostics in one control system. The system uses two-out-of-three voting to provide high-integrity, error-free, uninterrupted process operation with no single point of failure.

The TRICON controller uses three identical channels; each channel independently executes the control program in parallel with the other two channels. Specialized hardware/software voting mechanisms qualify and verify all digital inputs and outputs from the field, while analog inputs are subject to a mid-value selection process. Because each channel is isolated from the others, no single-point failure in any channel can pass to another. If a hardware failure does occur on one channel, the other channels override it. Meanwhile the faulted module can be removed and replaced while the controller is online without interrupting the process.

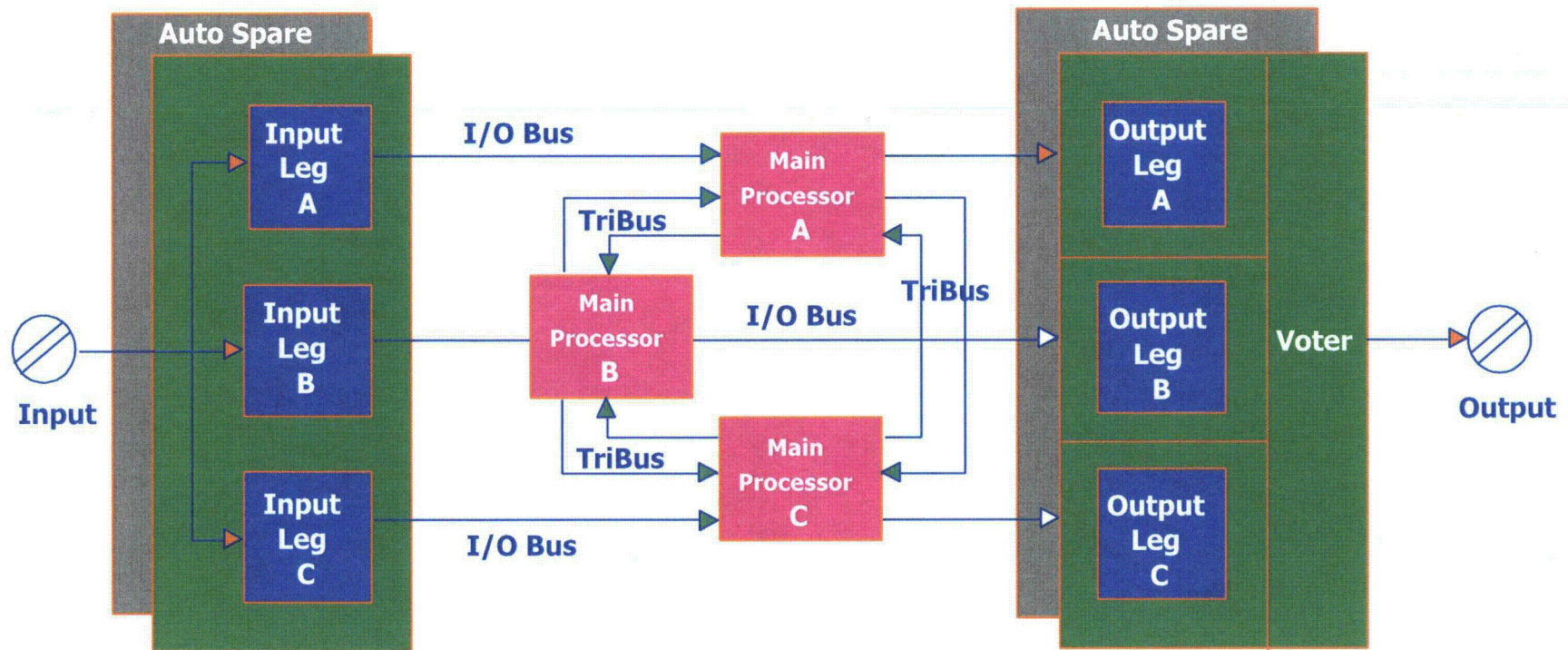
From the user's point of view, the TMR architecture is "transparent" in that application logic operates as a single control system. Similarly the input and output signals (sensors and actuators) are terminated at a single location that is available to all three processing channels (and electrically isolated between those channels).

The TMR redundancy of the individual TRICONs is used by the ESBWR to make each of the four divisions reliable for both actuation and to prevent inadvertent actuation; the redundancy required by Reference 7 is provided by the ESBWR's four independent Q-DCIS divisions.

The TRICON provides extensive diagnostics on each channel, module, and functional circuit and can immediately detect and report faults to the operator by means of indicators or alarms. All diagnostic fault information is accessible by the application program and the operator. The program or the operator can use diagnostic data to modify control actions or direct maintenance procedures.

The diagnostics are important in that a fault-tolerant control system must identify and compensate for failed control system components or elements and allow repair while continuing an assigned task without process interruption. The extremely high reliability of the TRICON, in addition to its high component quality is also dependent on identifying faults and repairing them in a reasonable time to minimize the chances of receiving a second fault while the first is extant.

Figure 3-1 TRICON TMR Processing Configuration



The TRICON is specifically designed to support applications having the highest reliability requirements. Other key features of the TRICON controller that ensure the highest possible system integrity are:

- No single point of failure
- Ability to operate with 3, 2 or 1 main processors before shutdown
- Fully implemented and transparent triplication
- Comprehensive system diagnostics
- Complete range of I/O modules
- Remote I/O up to 7.5 miles (12 kilometers) from the main processors
- Simple, online module repair

Figure 3-2 depicts the TRICON main chassis that is distinguished by housing the three main processors. In the ESBWR application there is a main chassis/three main processors for each of the four SSLC/ESF divisions. All TRICON chassis use redundant power supplies and redundant power feeds and can operate on either. In addition to the main processors and power supplies, the TRICON main chassis provides slots to accommodate I/O modules (data acquisition) and communication modules as required for the application. Once the location and type of cards are finalized, the chassis can be “configured” such that only the correct card type can be inserted into a particular slot.

3.2 EXPANSION/REMOTE DATA ACQUISITION

The TRICON system provides for data acquisition remote from the main chassis (i.e. the chassis containing the main processors); the capability is illustrated in Figure 3-3. The simplest way to accommodate additional signals is to use an “expansion” chassis that is connected to the main chassis by copper wire (the connector positions are at the upper left of Figure 3-2). The use of copper connecting cable is acceptable within the same division but there is a distance limitation that usually restricts the location of the expansion chassis to within the same cabinet, a nearby cabinet or a cabinet in a nearby room. This capability is used within both the RB and CB.

Additionally the main (or expansion) chassis may be connected to an “RXM” chassis (refer to Figure 3-3) which is, in turn, connected to another RXM chassis which can be located considerably further away than an expansion chassis since the RXM chassis are interconnected with fiber. This technique is used within a division for chassis located in different (RB and CB) buildings. In all cases the triple redundancy of the TRICON is carried through to the remote data acquisition.

3.3 DATA ACQUISITION

Q-DCIS input and output signals require 4 – 20 ma analog input capability, thermocouple input capability, dry contact and voltage change discrete input capability (control switches and process switches), and discrete output capability (squibs, solenoids and status information).

Figure 3-2 TRICON Main Chassis

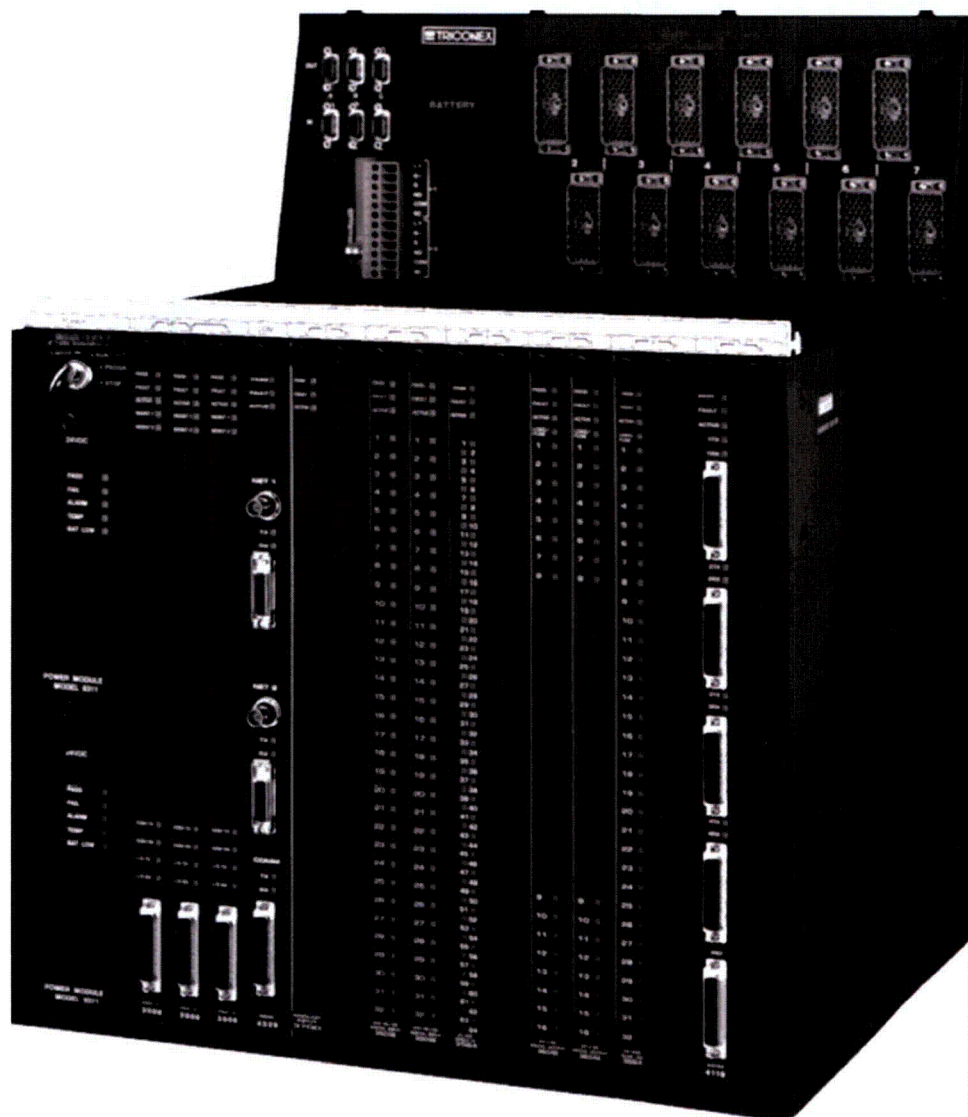
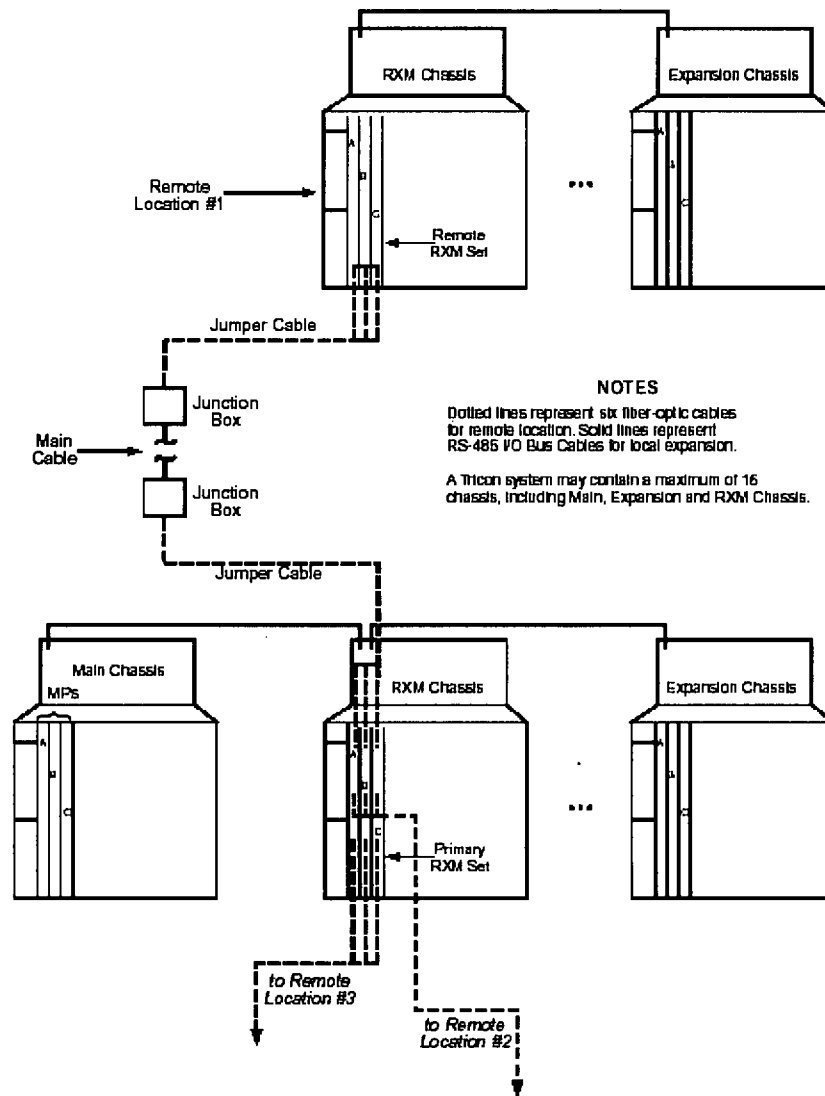


Figure 3-3 TRICON Expansion Capability



The available TRICON input/output capabilities include:

- Digital Input (DI) Modules that receive discrete signals at these nominal voltages: 115 VAC/VDC, 48 VAC/VDC, and 24 VAC/VDC. All voltages are available in TMR modules. Non-TMR modules are available in 24 VDC and 48 VDC only.
- Supervised Digital Output (SDO) Modules that produce discrete output signals of these nominal voltages, with diagnostic coverage of the field circuit and load device: 115 VAC, 120 VDC, 48 VDC, and 24 VDC.
- Digital Output Modules that produce discrete output signals at these nominal voltages: 115 VAC, 120 VDC, 24 and 48 VDC. Dual output modules are also available. If required by HFE, non-TMR dry contact relay output modules are available for annunciator panels.
- Analog Input Modules that receive analog signals of these types: 0-5 VDC, 0-10 VDC and Thermocouple types J, K, T and E. These are available in both isolated and DC-coupled versions.

3.4 COMMUNICATION

The TRICON has several modules available for the various chassis but the ESBWR application uses the TRICON Communication Module (TCM) that enables a TRICON controller to communicate with Modbus devices (masters or slaves), a network printer, a TriStation personal computer (for initial setup), other Triconex controllers, and other external devices on Ethernet networks; only the latter three applications are used for the ESBWR. Each TCM has four serial ports, two Ethernet network ports, and one debug port (for Triconex use). A single TRICON controller supports up to four TCMs, which reside in two logical slots (four physical). This arrangement provides a total of sixteen serial ports and eight Ethernet network ports.

4.0 APPLICATION

This section describes the actual TRICON hardware and software ESBWR configuration used to meet SSLC/ESF requirements and capabilities.

The Q-DCIS consists of the NUMAC hardware/software platforms that include RPS (including MSIV isolation), the NMS and anticipated transients without scram (ATWS)/SLCS) and the TRICON hardware/software platform for SSLC/ESF. These systems and their associated sensors are organized into four divisions. The touch screen displays associated with each division provide for the control of the safety-related equipment and additionally provide process and diagnostic alarms and the necessary monitoring of the plant safety-related functions during and following an accident, as required by Reference 11.

4.1 COMMON Q-DCIS APPLICATION AND OVERVIEW

4.1.1 General Data and Electrical Isolation

Figure 1-2 is a schematic view of the ESBWR DCIS with the safety-related DCIS (Q-DCIS) that includes both the NUMAC and TRICON hardware/software platforms shown in the lower left. The N-DCIS is emphasized in Figure 1-2 to indicate that the Q-DCIS is isolated from the outside world by the plant firewall used to implement the hardware portions of the cyber security plan. The Q-DCIS is further isolated from the outside world by the workstations between the unit and plant data highways (the former is the plant monitoring and control network and the latter is used for printers, internal engineering workstations and the firewall that sends data one way from the plant nuclear data link (NDL), technical support center (TSC), emergency offsite facility (EOF), simulator, and utility owned data systems. The point is to emphasize that it is highly unlikely that the safety-related networks can be accessed (much less affected) by the outside world.

Within the plant nonsafety-related monitoring and control network, gateways are used between the Q-DCIS systems and the N-DCIS systems. The gateways are nonsafety-related workstations used to translate (not isolate) the Q-DCIS information sent to N-DCIS. The four divisional TRICONs each have their own gateway and all Q-DCIS to N-DCIS communication is by fiber. There are no electrical connections between Q-DCIS and N-DCIS. The only points of access to the Q-DCIS are these gateways and they are set up to receive only safety-related data with two exceptions. The first is the average power range monitor (APRM) and local power range monitor (LPRM) calibration data that can only be accepted by the NUMAC NMS when the division has been manually made inoperable as a deliberate operator action; there are no comparable data sent to the TRICONs. The second data type is time-of-day used by both the TRICONs and NUMACs to time tag safety-related data sent to N-DCIS for recording and analysis and to indicate “real time” on the TRICON displays. The time signals are never used to synchronize the divisions nor as an input to any SSLC/ESF logic.

Electrical isolation and data isolation between divisions and between Q-DCIS and N-DCIS is accomplished within the division, respectively the communications interface module (CIM) in the NUMACs and the TCM in the TRICONs; these components are safety-related. Data isolation is entirely within the Q-DCIS and is independent of the ability of the N-DCIS firewall to operate correctly.

4.1.2 General Logic Configuration

The primary responsibility of the SSLC/ESF system logics is to initiate ECCS or isolations; this requirement is illustrated in Figure 4-1. Each of the four divisions has its own independent sensors that are powered by that division. The sensor outputs are compared with setpoints and each division independently makes a decision to trip (isolate or actuate). The trip decision is sent (via fiber) to the other three divisions.

Each SSLC/ESF division has a bypass unit that is driven from a common (to the four divisions) fiber optic switch that physically allows only one division at a time to be bypassed. Each division bypass unit provides the divisional bypass status to its own division and, via fiber, to the other three divisions.

The trip decisions and divisional bypass status are sent to two-out-of-four logic; this logic produces a trip if any two of the same divisional unbypassed parameters exceed their trip setpoint. The divisional bypass also disables its divisional trip output.

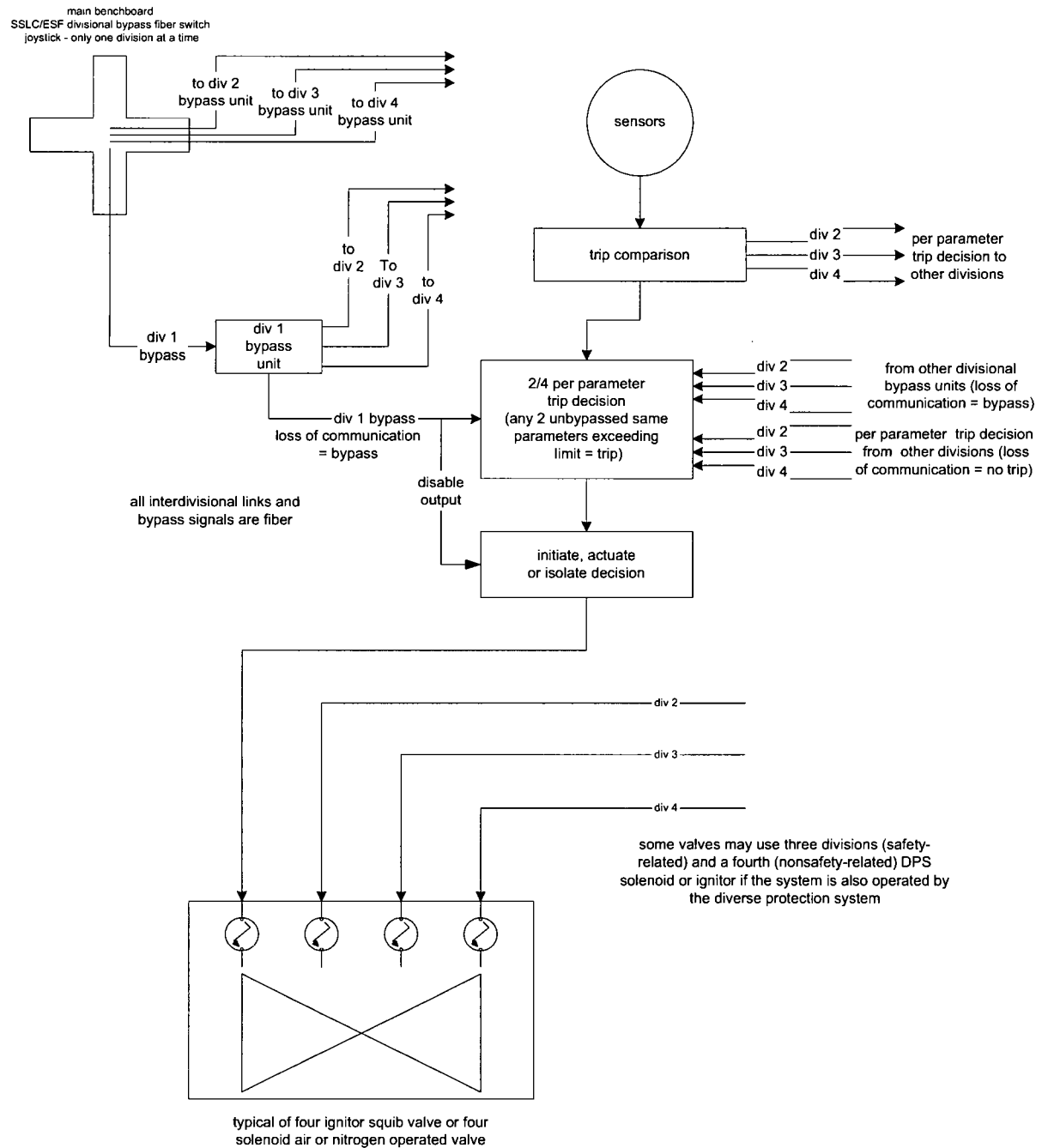
Previously designed nuclear power plants with active safety systems by definition had isolated (between divisions) ECCS actuators, a motor operated valve (MOV) or ECCS pump or fan with an actuator (motor) that could only be connected to one division (even if the actuating logic was cross divisional). Such plants in the United States were generally designed as “N-1” which referred to the ability to meet the safety requirements with one division failed or out of service.

The ESBWR is a passive plant that does not use active MOVs, pumps or fans (with two exceptions, namely, the MCR emergency filtration unit fans and the containment post-accident fans); instead the ECCS systems are actuated with squibs (propellant ignitors) and solenoids. Figure 4-1 indicates the simplified ECCS systems/actuators of the ESBWR.

The ECCS squib valves (GDCS and ADS DPVs) and the process isolation valves (LD&IS), SRVs (ADS), and initiation valves (ICS) are each fitted with at least four actuators (ignitors or solenoids) – any one of which can perform the required safety function (fire and open for squibs, open for actuating valve solenoids and close for process isolation valves). For example, there are eight DPVs (squib actuated valves used to depressurize the reactor for GDCS), each of which has four ignitors with each ignitor connected to a different division. Any single division can open the DPV which allows the plant to be designed as “N-2” because any two (of four) divisions are all that is necessary to accomplish the safety-related trip and ECCS functions. N-2 allows one division to be taken out of service or inoperative, another to have a random single divisional failure, and addresses a design basis event with the remaining division(s). N-2 also allows the ESBWR design to make inadvertent actuations of ECCS less likely since any of the four (three) divisions can operate the ECCS.

Figure 4-1 ESBWR SSLC/ESF Logic Architecture

division 1 – typical of four divisions



N-2 requires that only three of the four divisions be connected to any actuator (squib or solenoid valve); advantage is taken in most ECCS actuators by using three safety-related divisions and connecting the fourth squib or solenoid to the DPS, described in Chapter 7 of Reference 1; the DPS is designed to address the very unlikely common cause failure (CCF) of the TRICON (and NUMAC) hardware/software platforms by performing a subset of parallel RPS, isolation and ECCS functions even if the SSLC/ESF is completely inoperable.

Table 4-1 provides an example of how the DPVs are allocated to the four divisions and DPS such that the divisions remain symmetrical and all ECCS actuators are operable.

Table 4-1 Example Assignment of DPV Squib Valve Ignitors to SSLC/ESF and DPS

DPV	1 st ignitor	2 nd ignitor	3 rd ignitor	4th ignitor
F004A	div 1	div 2	div 3	DPS
F004B	div 2	div 3	div 4	DPS
F004C	div 3	div 4	div 1	DPS
F004D	div 4	div 1	div 2	DPS
F005A	div 1	div 2	div 3	DPS
F005B	div 2	div 3	div 4	DPS
F005C	div 3	div 4	div 1	DPS
F005D	div 4	div 1	div 2	DPS

Unlike the RPS and MSIV LD&IS NUMAC hardware/software platform design, the SSLC/ESF is designed not to be “fail safe”; an operator bypass or a self diagnosed fault alarms and disables the divisional trip outputs. To support this concept, loss of communication from the TRICON RMUs (expansion and RXM chassis) is interpreted as “fail as is”. Similarly the loss of signal from the bypass switch is treated as “bypass” with the caveat that further logic ensures that more than one division in bypass results in “no bypass” (indication of more than one division in bypass can only occur with loss of communication or other bypass unit failures since it is not physically possible from the bypass switch itself).

4.1.3 Diversity

The diversity used in the ESBWR DCIS (Reference 12) is summarized here in Figure 4-2; within the Q-DCIS, the RPS, LD&IS (MSIV) and NMS use NUMAC hardware and software different from the SSLC/ESF TRICON processors. In turn both the RPS/NMS and SSLC/ESF DCIS systems use hardware and software platforms different from the N-DCIS systems, specifically including the DPS, which provides a completely diverse backup design to most protection functions in the Q-DCIS. The severe accident BiMac deluge system is also diverse from both Q-DCIS and N-DCIS.

Figure 4-2 Hardware/Software (Platform) Diversity

Safety	Safety-Related		Nonsafety-Related				
Category	Q-DCIS		N-DCIS				
System Families	RPS NMS	SSLC/ESF	DPS	Nuclear Control Systems	Other N-DCIS Systems	PCF	Severe Accident
Architecture	NUMAC	TRICON	MK6e (TMR)**	MK6e (TMR)**	MK6e (dual redundant)	Workstations	PLCs
Systems/Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLCS*	ICS ADS GDCS SLCS LD&IS (non MSIV)	RPS SSLC/ESF LD&IS backup	FWC, SB&PC, T/G Control, PAS (automación)	PIP A, PIP B, Balance of Plant (power generation)	HMI (VDUs), Alarm Management SPDS, Historian, 3D Monicore	Deluge System (GDCS subsystem)

Diversity Strategy

* non programmable diverse from RPS hardware/software

** triple modular redundant

Within Safety-Related Controls

Safety-Related vs DPS

Safety-Related vs Nonsafety-Related

Figure 4-3 ESBWR Systems Diversity

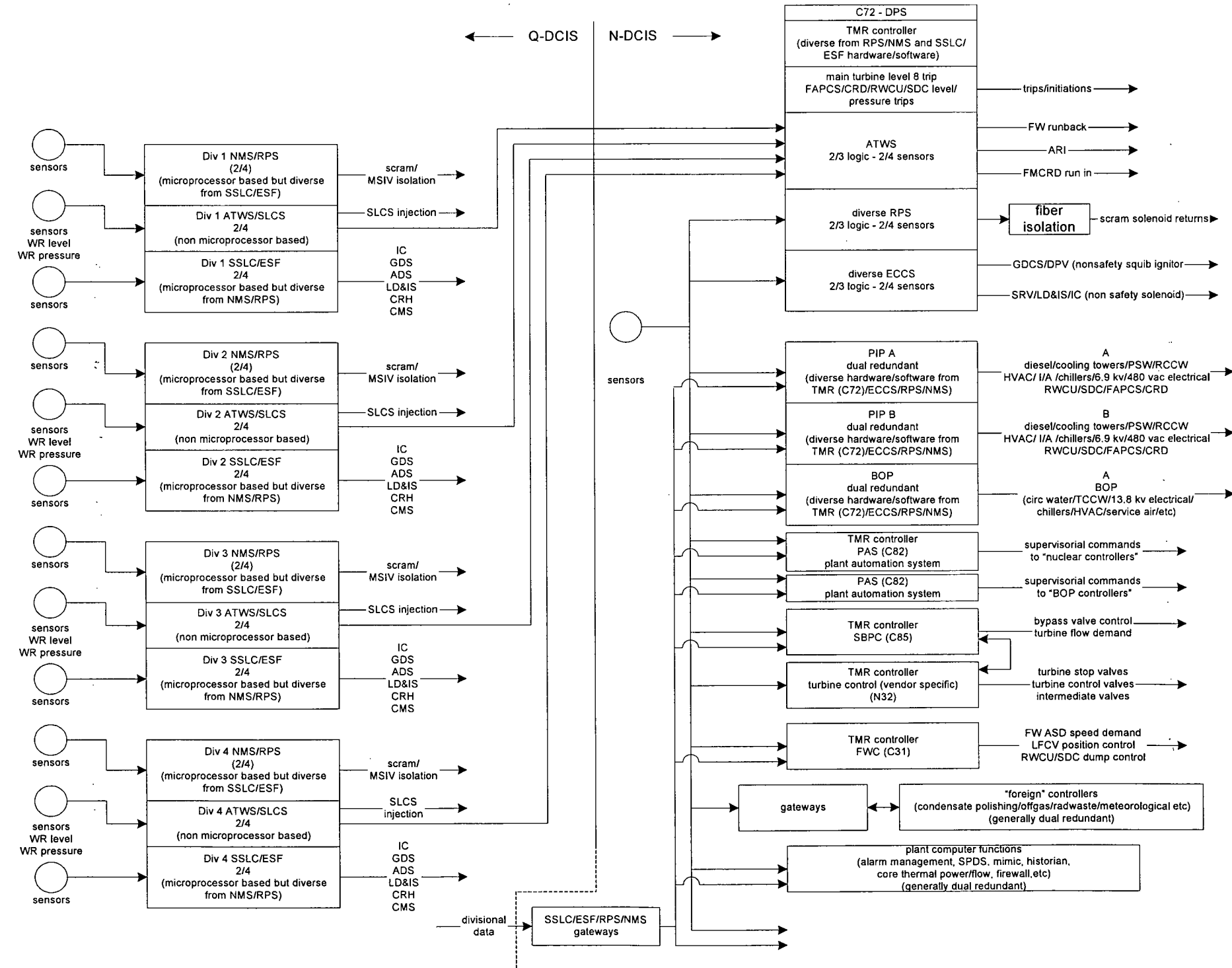


Figure 4-4 ESBWR Q-DCIS Power

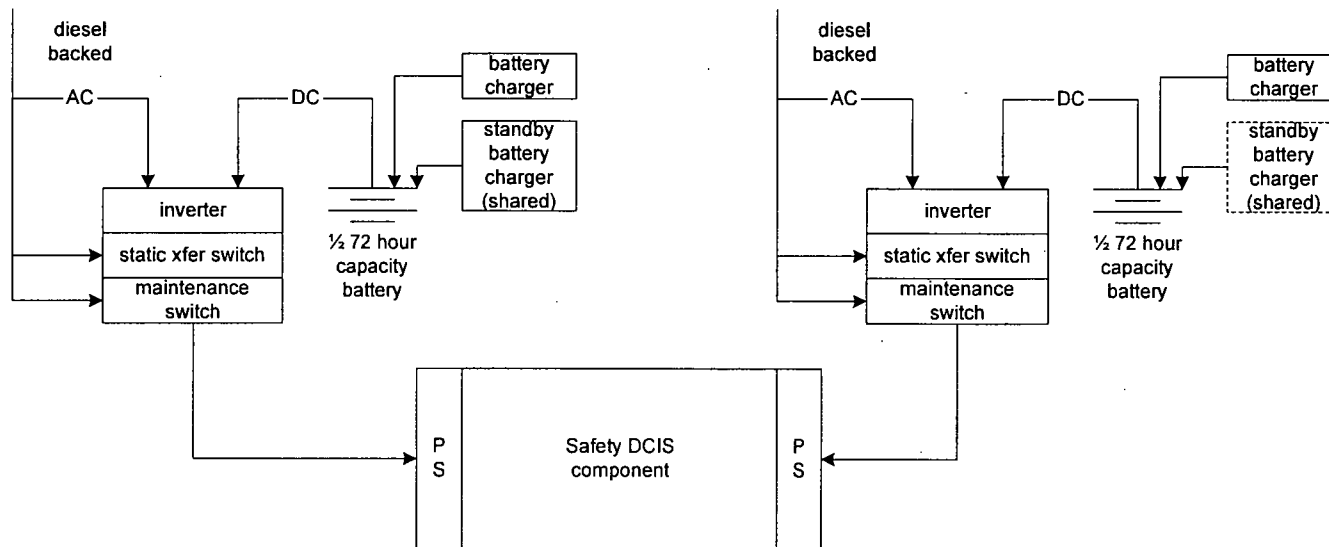
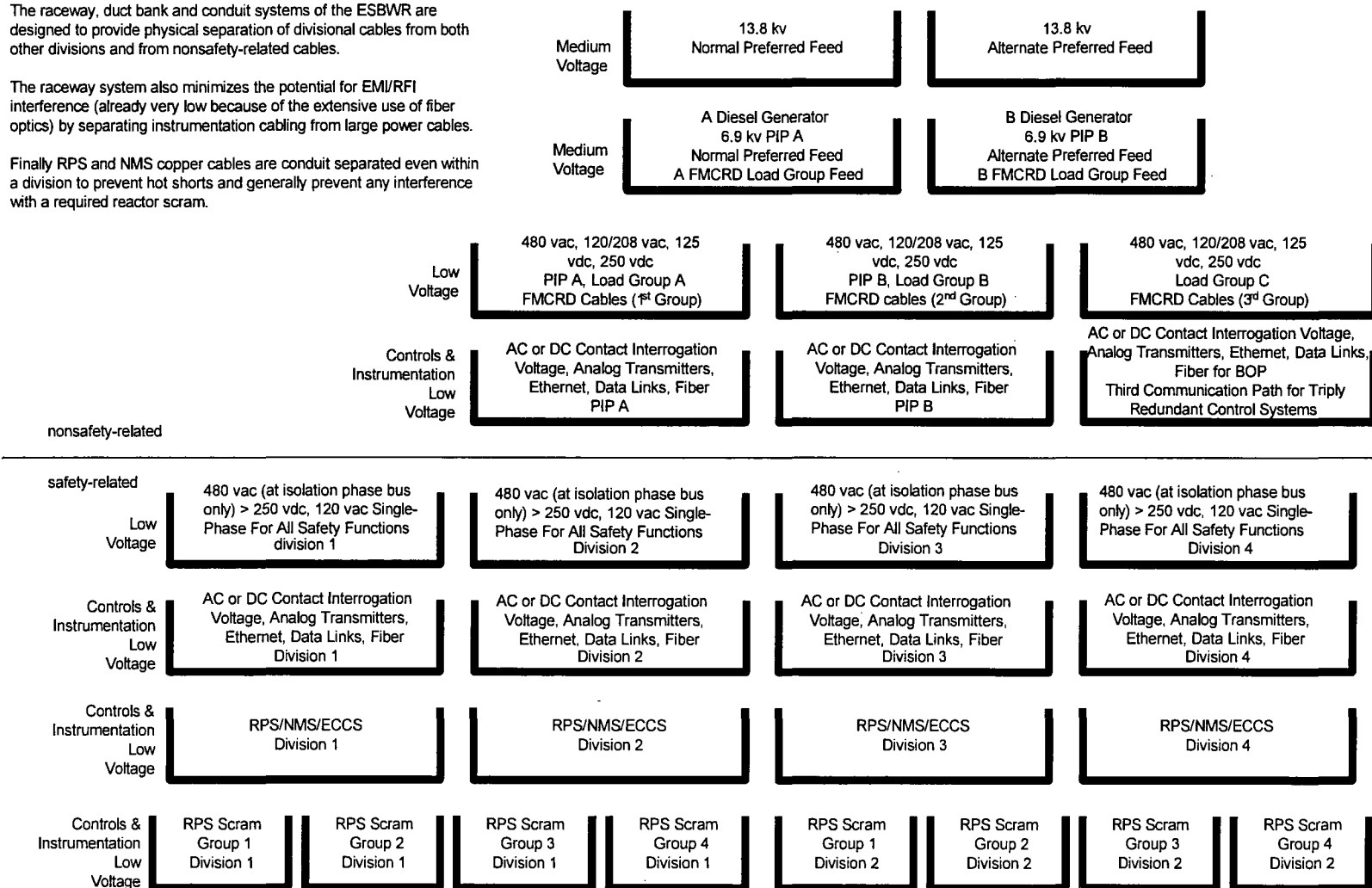


Figure 4-5 ESBWR DCIS and POWER Separation

The raceway, duct bank and conduit systems of the ESBWR are designed to provide physical separation of divisional cables from both other divisions and from nonsafety-related cables.

The raceway system also minimizes the potential for EMI/RFI interference (already very low because of the extensive use of fiber optics) by separating instrumentation cabling from large power cables.

Finally RPS and NMS copper cables are conduit separated even within a division to prevent hot shorts and generally prevent any interference with a required reactor scram.



On the N-DCIS side, the important nuclear I&C systems, such as DPS, use triply redundant controllers to improve their reliability for power generation and, in the case of DPS, to provide reliability for both the backup SCRAM and ESF/ECCS functions and to prevent inadvertent actuations.

Figure 4-3 indicates systems and sensor relationships between the various I&C systems.

4.1.4 Power

All Q-DCIS components and cabinets are redundantly powered as indicated in Figure 4-4. The various Q-DCIS actively powered equipment (specifically including the TRICON) have two power supplies and two 120 VAC uninterruptible power feeds; although normally component power requirements are shared between the two supplies/feeds, either is capable of independently operating the component. Ultimately each power feed is traceable to one of the two safety-related inverters per division that, in turn, are normally powered by offsite power or either of the two diesel generators. For design basis events that include SBO, the inverters are each powered by their own safety-related battery. The two batteries and inverters together can supply the division for 72 hours; if one of the batteries or inverters or two (of three) chargers are inoperable the division is considered out of service – however the only functionality lost is time since the single remaining battery can only operate the division during an SBO for approximately 36 hours. The power supplies, power feeds, inverters, chargers and batteries are monitored continuously and alarmed by both the Q-DCIS and N-DCIS. Although the division is considered inoperable with a failed power supply, the operator does not have to put it in bypass.

4.1.5 Separation

Per division the NUMAC RTIF and NMS cabinets and the SSLC/ESF TRICON main processor cabinets are located in separate Q-DCIS rooms in the control building (CB); these rooms are in fire zones separate from each other and from the N-DCIS rooms and from the MCR. The Q-DCIS cabinets per division are also physically separated from each other in the reactor building (RB); these include the NUMAC and TRICON RMUs (in the TRICON case these are actually the expansion chassis and RXM chassis).

As indicated on Figure 4-5 all cabling within a division is kept physically separate from other divisions and nonsafety-related cabling. Only fiber is used to communicate between divisions and between divisions and N-DCIS. No physical event affecting one division is able to affect another division. Because of the inherent security of the communications schemes, no MCR event or remote shutdown system (RSS) panel event is able to cause inadvertent operation of any safety-related or nonsafety-related equipment.

4.2 SPECIFIC SSLC/ESF APPLICATION

The specific application of the TRICON to the SSLC/ESF is discussed in the following subsections.

4.2.1 TRICON Configuration

The four divisions of TRICON (SSLC/ESF) are arranged as shown in Figure 4-6. The design includes the main processors in the CB, a network to support two out of four logic, a data link to the NUMACs to allow their parameters to be displayed and alarmed on safety-related VDUs, the VDUs that support both safety-related monitoring and control and a data link to the N-DCIS for

monitoring, recording, and alarming – but not control. The four divisions are both electrically and data isolated from one another and the N-DCIS.

Details of the configurations are discussed in the following subsections.

4.2.2 Location

All Q-DCIS components (except the RPS sensors in the turbine building) are located in the RB and CB as indicated in Table 4-2. One elevation of the CB has four physically separated Q-DCIS rooms housing the four divisions of NUMAC (RPS, NMS, process radiation and ATWS/SLC) and TRICON (SSLC/ESF main chassis) cabinets. The MCR houses four divisions of VDUs, fiber and hard wired switches, but the MCR is in a fire zone and habitability area separate from the Q-DCIS rooms; the equipment in the latter rooms operate independently of MCR status, specifically during fires.

The RB is organized divisionally into physically separate quadrants. The Q-DCIS components are appropriately located in these quadrants at various elevations. The RB houses the TRICON (SSLC/ESF) RXM and expansion chassis that are connected via triply redundant fiber (per division) to the main chassis in the CB Q-DCIS rooms. The RB additionally houses the two RSS panels on which are mounted division 1 and 2 VDUs. These VDUs operate independently of the MCR VDUs and allow the operator to monitor and control any division 1 and 2 process as he would from the MCR.

4.2.3 Per Division SSLC/ESF arrangement

The TRICON cabinets for each division are indicated in Figures 4-7 through 4-10. The divisions are symmetrical except that divisions 1 and 2 have additional RB data acquisition needed to acquire the fine motion control rod drive (FMCRD) separation switches (used to block rod motion and provide safety-related separation alarms). Also divisions 1 and 2 have two additional VDUs (one per division) on each of the RSS panels.

The cabinet locations are chosen to be near areas of high signal “density”; these include elevations where penetrations to the reactor containment exist, areas with instrument racks and safety-related electrical equipment and FMCRD cabling. The precise number of cabinets cannot be stated until the final safety-related signal list is complete but the current design has room for additional TRICON expansion cabinets that may be necessary. Additionally the module types and locations shown in the configuration drawings are subject to change until the signal list is finalized.

Figure 4-6 SSLC/ESF (TRICON) Configuration

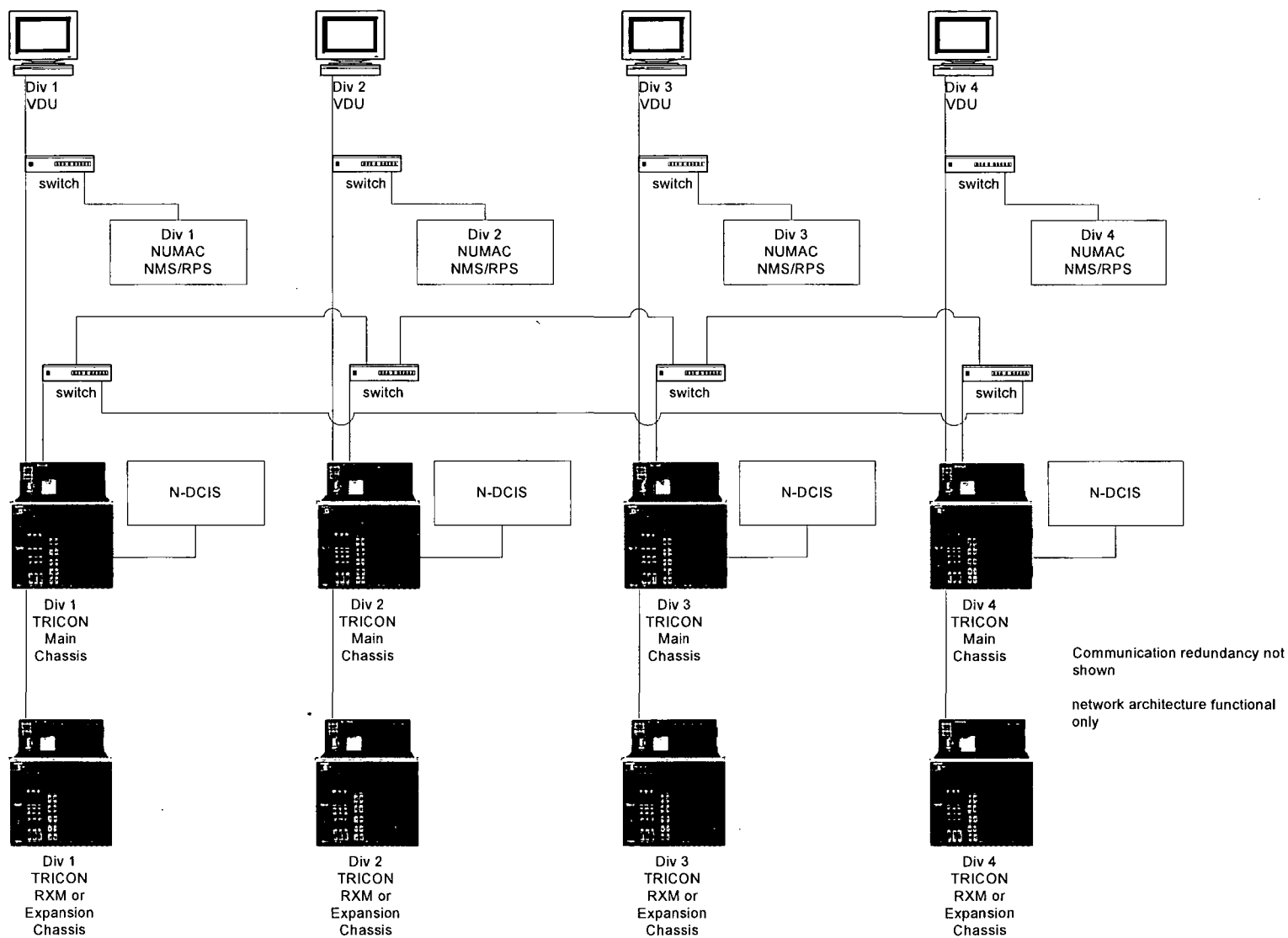
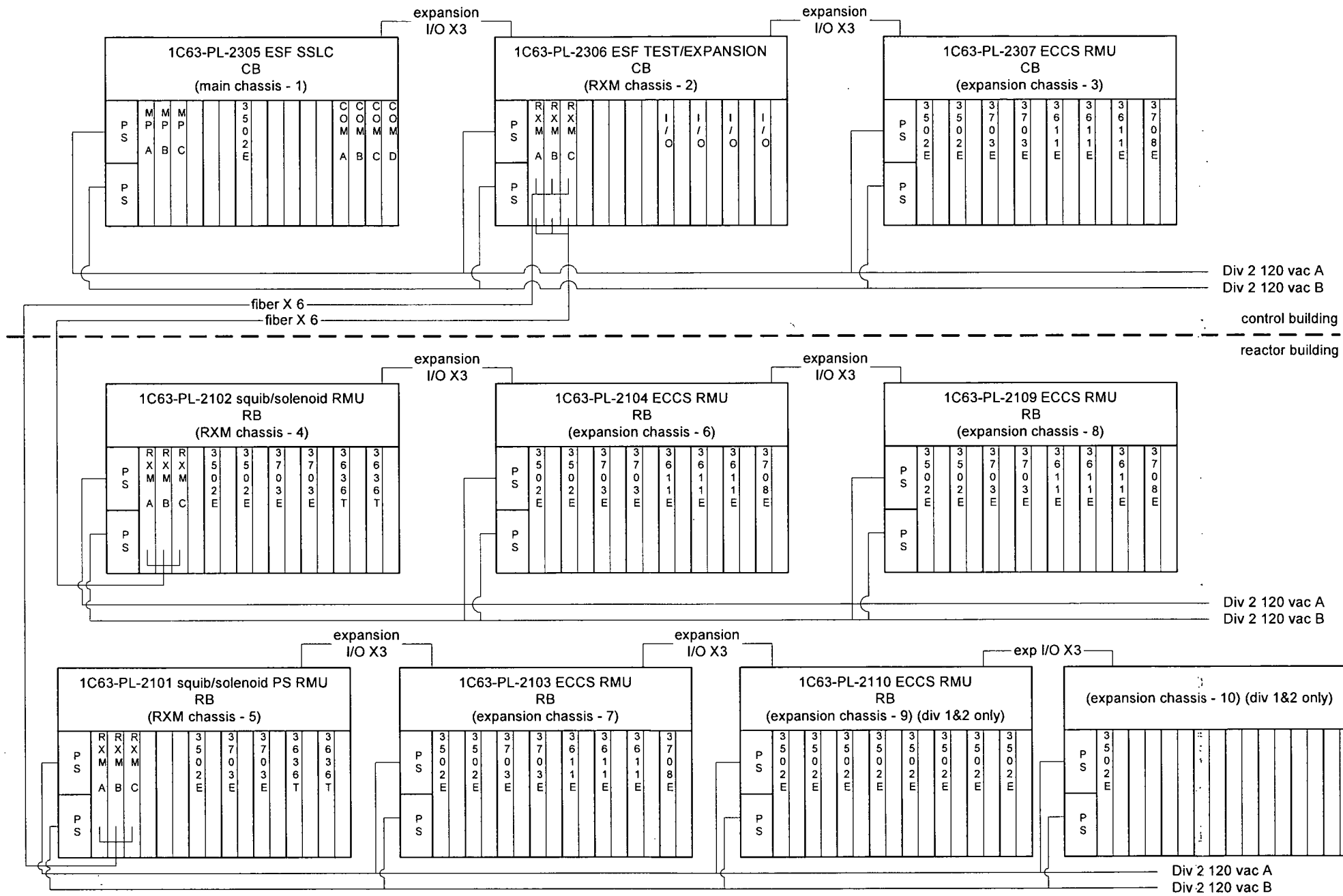


Table 4-2 SSLC/ESF Plant Locations

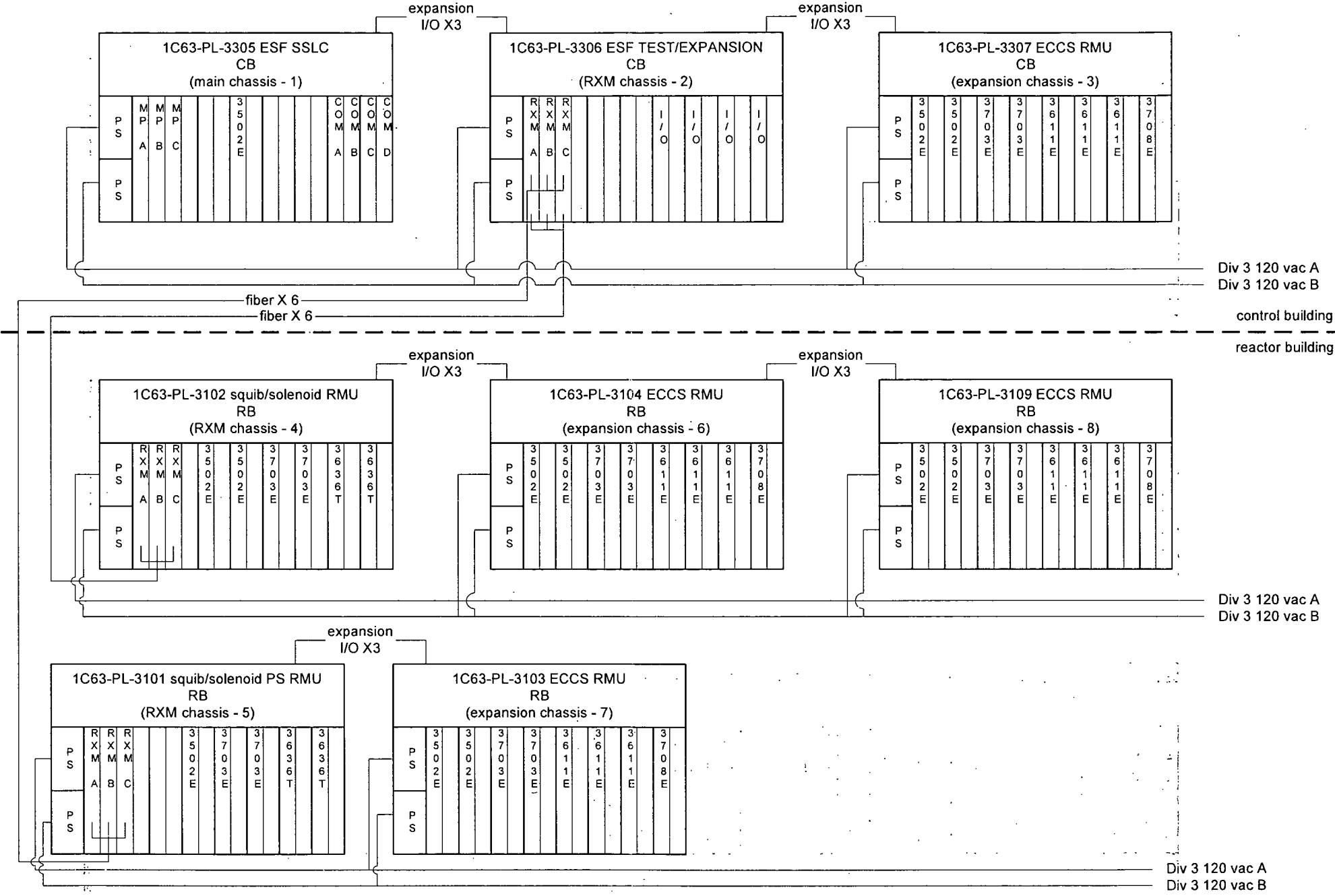
<i>Cabinet/chassis</i>	<i>Div 1</i>	<i>Div 2</i>	<i>Div 3</i>	<i>Div 4</i>	<i>function</i>
main chassis	C63-PL-1305 CB	C63-PL-2305 CB	C63-PL-3305 CB	C63-PL-4305 CB	main processors
RXM chassis	C63-PL-1306 CB	C63-PL-2306 CB	C63-PL-3306 CB	C63-PL-4306 CB	data acquisition RXM chassis
RMU chassis	C63-PL-1307 CB	C63-PL-2307 CB	C63-PL-3307 CB	0 C63-PL-4307 CB	fiber extension to RB expansion chassis data acquisition
RMU chassis	C63-PL-1102 RB	C63-PL-2102 RB	C63-PL-3102 RB	C63-PL-4102 RB	data acquisition RXM chassis
RMU chassis	C63-PL-1104 RB	C63-PL-2104 RB	C63-PL-3104 RB	C63-PL-4104 RB	fiber extension to CB expansion chassis data acquisition
RMU chassis	C63-PL-1101 RB	C63-PL-2101 RB	C63-PL-3101 RB	C63-PL-4101 RB	data acquisition RXM chassis
RMU chassis	C63-PL-1103 RB	C63-PL-2103 RB	C63-PL-3103 RB	C63-PL-4103 RB	fiber extension to CB expansion chassis data acquisition
RMU chassis	C63-PL-1109 RB	C63-PL-2109 RB	C63-PL-3109 RB	C63-PL-4109 RB	expansion chassis data acquisition
RMU chassis	C63-PL-1110 RB	C63-PL-2110 RB			expansion chassis data acquisition for FMCRD separation switches
VDU	MCR	MCR	MCR	MCR	two VDUs per division
VDU	RSS	RSS			one VDU per division

Figure 4-8 Division 2 SSLC/ESF (TRICON) Configuration



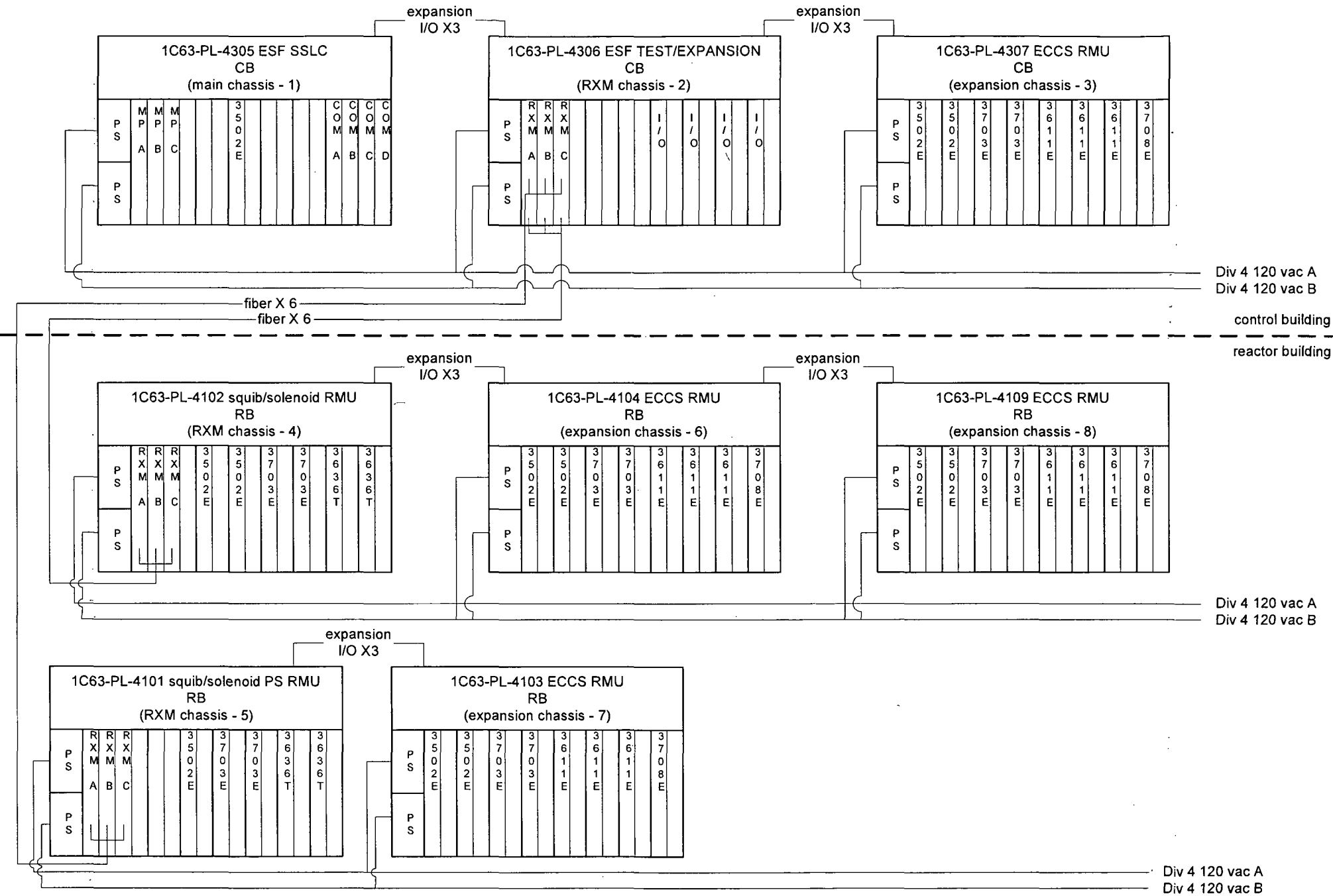
Notes:
all cabinets shown powered with redundant R13 (vital AC) power
all connections fiber unless otherwise indicated

Figure 4-9 Division 3 SSLC/ESF (TRICON) Configuration



Notes:
all cabinets shown powered with redundant R13 (vital AC) power
all connections fiber unless otherwise indicated

Figure 4-10 Division 4 SSLC/ESF (TRICON) Configuration



Notes:
all cabinets shown powered with redundant R13 (vital AC) power
all connections fiber unless otherwise indicated

4.2.4 Standard Data Acquisition

The SSLC/ESF functions require that each division be able to measure plant parameters such as pressure, level, radiation, voltage changes, process switches (dry contacts), temperatures and differential pressures. The TRICON system provides appropriate I/O cards as needed to acquire 4 – 20 ma, thermocouple, and analog voltages; similarly the TRICON system can excite dry contacts and monitor voltage changes.

4.2.4.1 Analog inputs

An analog input module includes three independent input channels. Each input channel receives variable voltage signals from each point, converts them to digital values, and transmits the values to the three main processor modules on demand. In TMR mode, one value is then selected using a mid-value selection algorithm to ensure correct data for every scan. Sensing of each input point is performed in a manner that prevents a single failure on one channel from affecting another channel. Each analog input module performs complete, ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the Fault indicator for the module, which in turn activates the chassis alarm signal. The module's Fault indicator merely reports a channel fault, not a module failure—the module can operate properly with as many as two faulty channels.

Analog input modules support hot spare capability that allows online replacement of a faulty module. The analog input module requires a separate external termination panel (ETP) with a cable interface to the TRICON backplane. Each module is mechanically keyed for proper installation in a TRICON chassis.

A thermocouple (TC) input module includes three independent input channels. Each input channel receives variable voltage signals from each point, performs TC linearization and cold-junction compensation, and converts the result to degrees Celsius or Fahrenheit. Each channel then transmits 16-bit signed integers representing 0.125 degrees per count to the three main processors on demand. In TMR mode, a value is then selected using a mid-value selection algorithm to ensure correct data for every scan. Each TC input module is programmable to support one TC type, selected from J, K and T for standard TC input modules and from J, K, T and E for isolated TC input modules.

The isolated TC input module allows users to select upscale or downscale burnout detection with the TriStation (setup) software. For non-isolated modules, upscale or downscale burnout detection depends on the field termination selected.

Triplicated temperature transducers residing on the field termination panel support cold-junction compensation. Each channel of a TC input module performs auto-calibration using internal precision voltage references. On the isolated module, a faulting cold junction transducer is annunciated by a cold-junction indicator on the front panel.

Each module performs complete ongoing diagnostics on each channel. Failure of any diagnostic on any channel activates the Fault indicator, which in turn activates the chassis alarm signal. The module Fault indicator merely reports a channel fault, not a module failure. The module continues to operate properly with as many as two faulty channels. The TC input module supports hot-spare capability that allows online replacement of a faulty module. The TC input module requires a separate ETP with a cable interface to the TRICON backplane. Each module is mechanically keyed to prevent improper installation in a configured chassis.

The ESBWR logic generally uses type K thermocouples and isolated thermocouple input cards.

4.2.4.2 Discrete inputs

Each TMR DI module has three isolated input channels that independently process all data input to the module. A microprocessor on each channel scans each input point, compiles data, and transmits it to the main processors upon demand. The input data is then voted at the main processors just prior to processing to maximize its integrity. All critical signal paths are 100 percent triplicated for guaranteed safety and maximum availability. Each channel conditions signals independently and provides optical isolation between the field and the TRICON. All TMR digital input modules sustain complete, ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module Fault indicator that in turn activates the chassis alarm signal. The module Fault indicator points to a channel fault, not a module failure. The module is guaranteed to operate properly in the presence of a single fault and may continue to operate properly with some multiple faults.

Discrete input modules 3502E, 3503E, and 3505E can self-test to detect stuck-ON conditions where the circuitry cannot tell whether a point has gone to the OFF state. (Although not final, it is anticipated that the 3502E discrete input module with 48 VDC contact excitation will be used in the ESBWR application). Because most safety-related systems are set up with a de-energize-to-trip capability, the ability to detect OFF points is an important feature. To test for stuck-ON inputs, a switch within the input circuitry is closed to allow a zero input (OFF) to be read by the optical isolation circuitry. The last data reading is frozen in the I/O communication processor while the test is running. All TMR digital input modules support hot-spare capability, and require a separate ETP with a cable interface to the TRICON backplane. Each module is mechanically keyed to prevent improper installation in a configured chassis.

4.2.5 SSLC/ESF Discrete Outputs

The SSLC/ESF functions require that each division be able to provide outputs that will operate the ESBWR actuators whether automatically commanded by the logic or manually commanded by the operator. To the field circuitry the TRICON discrete outputs appear like a switch except that the switch responds to a two out of three vote of the three main processors and the switches include extensive diagnostics.

The TRICON SDO modules are designed to meet the needs of systems whose outputs remain in a single state for extended periods of time (in some applications, for years). An SDO module receives output signals from the main processors on each of three channels. Each set of three signals is then voted upon by a fully fault tolerant quadruplicated output switch whose elements are power transistors, so that one voted output signal is passed to the field termination. Each SDO module has voltage and current loop back circuitry coupled with sophisticated online diagnostics that verify the operation of each output switch, the field circuit and the presence of a load. This design provides complete fault coverage without the need to influence the output signal.

The modules are called “supervised” because fault coverage is extended to include potential field problems. In other words, the field circuit is supervised by the SDO module so that the following field faults can be detected:

- Loss of power or blown fuse
- Open or missing load

- A field short resulting in the load being energized in error
- A shorted load in the de-energized state

Failure to detect field voltage on any output point energizes the power alarm indicator. Failure to detect the presence of a load energizes the load alarm indicator. All SDO modules support hot-spare modules and require a separate ETP with a cable interface to the TRICON backplane. The discrete output TRICON modules anticipated for the ESBWR application are 3623 and 3624 used for 125 VDC and 24 VDC loads; these are the most likely voltages to be used for the ESBWR solenoids and squib ignitors.

Because the precise electrical characteristics of the squib ignitors have not been determined it is possible that their required firing currents may be higher than the discrete output module ratings. In this case and for cases where dry (instead of solid state) contacts are required, a TRICON interposing relay can be used. Each interposing relay provides an auxiliary contact connected to a DI module by means of a loop back cable to verify relay activation by the digital output module. Interposing relay panels use compact general purpose power relays for reliability and are compatible with the various TRICON discrete output modules.

The current ESBWR SSLC/ESF application does not use analog outputs, except for CCF detection.

The 3636R/T and the 3636TN Relay Output (RO) Modules are non-triplicated modules for use on non-critical points which are not compatible with “high-side” solid-state output switches. An example is interfacing with annunciator panels or where there is a concern about current ratings of the solid state switches. The relay output module receives output signals from the main processors on each of three channels. The three sets of signals are then voted, and the voted data is used to drive the 32 individual relays. Each output has a loopback circuit which verifies the operation of each relay switch independently of the presence of a load, while ongoing diagnostics test the operational status of the module. Failure of any diagnostic activates the Fault indicator, which in turn activates the chassis alarm. The relay output module comes with normally open contacts. It supports hot-spare modules and requires a separate ETP with a cable interface to the TRICON backplane. If the relay output modules are used for the ESBWR application, the squib and solenoid control circuitry described below is still applicable.

The SSLC/ESF TRICON application uses the above “standard” discrete outputs for diagnostics and hardwired signaling within a division (for example the SSLC/ESF SLC initiation output to the NUMAC ATWS/SLC chassis which ultimately controls SLC). One of the major tasks of SSLC/ESF is to operate the squib valves (DPV, GDCS) and the solenoid valves (SRV and process isolation). It is important to avoid inadvertent operation of an SRV but the ESBWR is unique in that the inadvertent operation of a DPV would lead to the uncontrolled depressurization of the RPV into the containment (as opposed to the suppression pool). Although the ESBWR SSLC/ESF design must be highly reliable to actuate squib and solenoid valves when necessary, it is also important to avoid inadvertent actuation of these valves.

The problem of inadvertent actuation is aggravated by the N-2 design of the ESBWR where any squib and solenoid valve can be actuated by any one of three SSLC/ESF divisions or the DPS or any one of four SSLC/ESF divisions. Inadvertent actuation is made less probable by the necessity for at least two divisions of logic being required for any division to operate the valve. This leaves only the possibility of single failures within the division and operator/technician error causing inadvertent actuation.

Figure 4-11 TRICON Cabinet C63-PL-X101 Detail

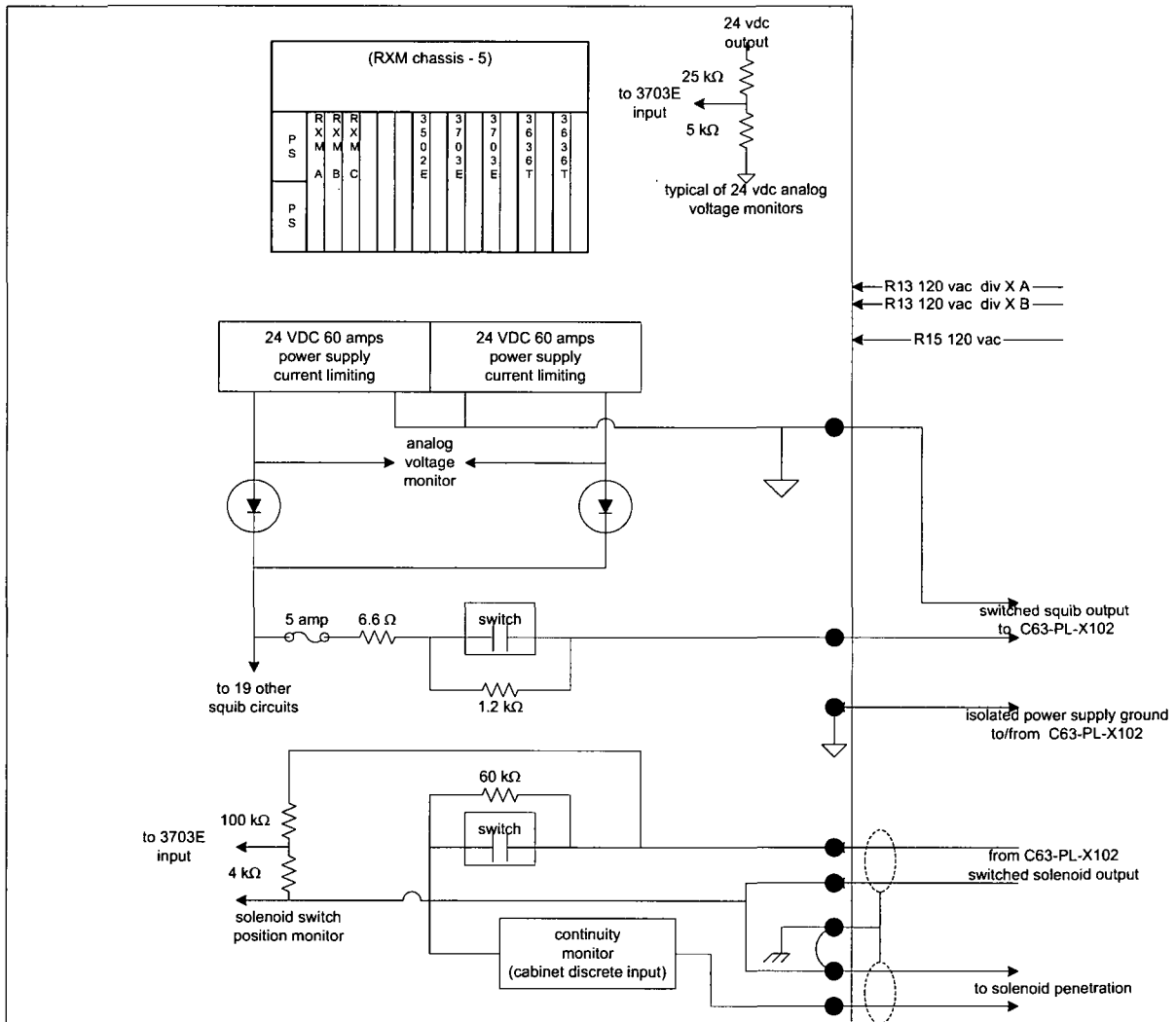
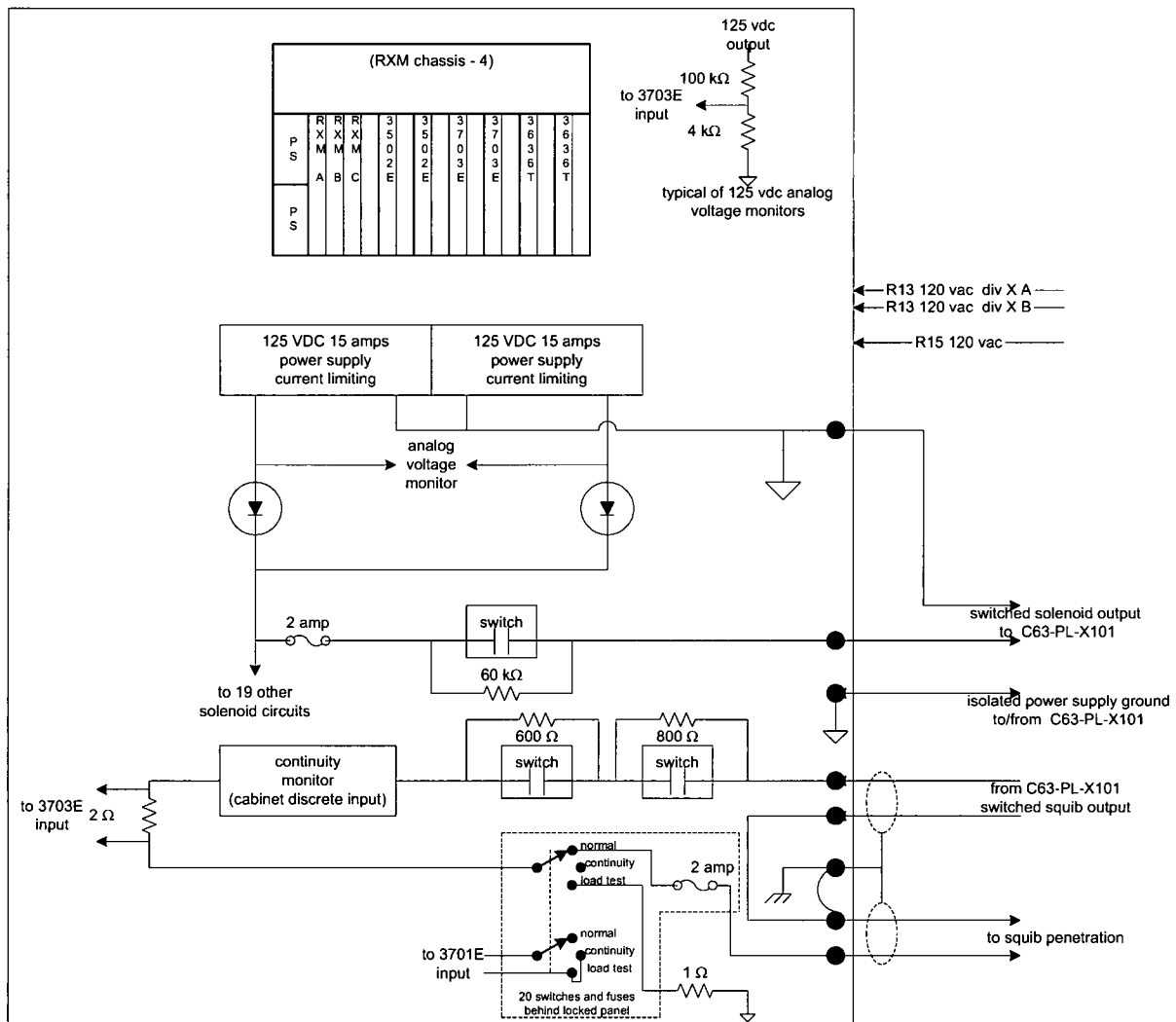


Figure 4-12 TRICON Cabinet C63-PL-X102 Detail



The TRICON application is specifically designed per division to avoid inadvertent actuation considering normal operation and surveillance; details are provided in Figures 4-11 and 4-12. Per division the scheme involves two RMUs (TRICON RXM chassis) that are physically located at different elevations of the RB. The SSLC/ESF application includes internal power supplies to operate the squib ignitors and solenoids instead of using the plant safety-related batteries directly. The reasons for this include:

- There are two batteries per division and in keeping with the DCIS design philosophy for internal divisional redundancy, it is desirable that the ECCS operates from either source.
- The use of internal power supplies ensures better regulation than the battery chargers can provide – a constant voltage source without electrical “spikes” minimizes the probability of inadvertent actuation.
- The use of internal power supplies allows (one side of) the solenoids and squib actuators to be grounded – this minimizes the possibility of the wire leads into containment acting like an antenna and thereby producing EMI/RFI causing inadvertent actuation. The power supplies also fix the maximum voltage to ground.
- Internal power supplies also allow monitoring and, if necessary, shutdown of the power supply to prevent inadvertent actuation.

The RMU cabinet (per division) on one RB elevation houses the redundant 24 VDC internal power supplies used for the squib initiators, while the RMU cabinet (per division) on a different RB location houses the redundant 125 VDC internal power supplies used for the SRV and process isolation valve solenoids (the power supply voltages may change as solenoids and squib ignitor requirements are finalized). In all cases each power supply is powered from one of the two 120 VAC uninterruptible power feeds to the cabinet and the outputs of the two supplies are gated to make a common output such that either supply/power feed can supply the squib ignitors/solenoids. The output of each individual power supply is monitored (by a TRICON analog input) before the diode gating such that the SSLC/ESF can alarm a power supply failure (even though no functionality is lost). The power supplies are over-voltage protected and current-limiting.

The logic for the squib ignitors differs slightly from the solenoid logic. The basic design for each squib ignitor logic is three switches in series between the power supply and the ignitor; one of the switches is in the cabinet on one elevation while the remaining two switches are in the cabinet on a different elevation. The division ignitor initiation logic is first that two of four divisions determine that initiation should occur (the determination is the result of a two out of three decision of the three TRICON main processors within the division). Then the voting logic in each of three separate discrete output modules must determine that two of three of the main processors commanded initiation. Overall the logic requires two of four divisions to initiate and within the division three simultaneous single failures must occur before a squib ignitor can be inadvertently fired. The location of the switches in two physically separated cabinets makes it very unlikely that a “hot short” or fire will cause inadvertent actuation.

The actual electrical circuit for an ignitor assumes that it will fire with two amps and that its electrical resistance is very small; when the final ignitor characteristics are known the power supply capabilities and component resistances in the following description may change but this will not affect functionality of the circuit. Additionally the circuit must accommodate the fact that a fired ignitor may either open or short circuit.

For each ignitor circuit the first component is a (nominal) 5 amp fuse followed by a current limiting resistor; the resistor is sized assuming that the ignitor shorts with the three series switches closed. The power supply is designed to support all of the ignitors shorting without lowering the power supply voltage and preventing another ignitor from firing.

Next in the ignitor circuit are the three series switches that are each paralleled by a resistor; each resistor has a different value. The next two components are a continuity monitor and a series resistor whose voltage is measured by a TRICON analog input. The resistors across the normally open switches ensure that there is always current in the loop that goes through the continuity monitor and squib ignitor; the current selected is well below the required ignitor firing current. The continuity monitor has an output contact that closes with current and this contact is monitored by a TRICON discrete input. This circuit continuously monitors the ignitor by providing an INOP alarm (Reference 9) if the circuit from the RMU through the containment penetration or the squib ignitor “open circuits” (note that this only disables one of the four ignitors on a valve such that ECCS functionality is not lost).

The purpose of the three different resistor values across the three switches is to allow surveillance of the individual switches one at a time. Closing each switch changes the monitoring current in the loop (as measured by the series resistor/TRICON input) and each closed switch changes the current differently. This scheme allow individual switch operability to be checked on-line and independently of the TRICON diagnostics without actually firing an ignitor.

The final components in the ignitor circuit are in a locked compartment of the RMU cabinet. The first is a double pole triple throw manual switch whose “normal” position completes the circuit to the squib ignitor through an accessible fuse. The center position of the switch is “continuity” and deliberately opens the ignitor circuit; its intent is to test the operability of the continuity monitor. The third switch position is “load test” which also disconnects the squib initiator but allows all three firing switches to be operated simultaneously and send their current through a “test” resistor. This demonstrates that the actual firing logic works and that the power supplies can provide the required firing current (as measured by the series resistor/TRICON input). The second pole of the switch is used to operate a TRICON discrete input that also provides an INOP alarm whenever the switch is in the “continuity” or “load test” position.

The accessible fuse (in the locked compartment) is available whenever the operator wants to absolutely prevent squib ignitor firing, for example, during troubleshooting or testing. Removing the fuse picks up the continuity monitor alarm.

The scheme for the SSLC/ESF solenoids is similar to the logic for the squib ignitors except that there are only two switches in series to operate a solenoid. For the case of the solenoid operated process isolation valves and SRVs, the consequences of an inadvertent actuation are not as severe since either power generation is only temporarily affected, or because the SRV discharges are routed by tailpipes to the suppression pool.

4.2.6 TRICON Communications

The ESBWR TRICON application requires four distinct types of communication. These include:

- Communication between divisions to support the safety-related VDUs and the two out of four ECCS initiation logic
- The TRICON to safety-related VDUs communication

- The TRICON to N-DCIS data sent through gateways
- The NUMAC NMS and RPS data sent to safety-related VDUs for display purposes

All of this communication is implemented using redundant fiber links and all communication is supported by redundant power supplies. Figures 4-13 through 4-16 indicate that all of the above communication is implemented using four TRICON communications modules per division located in the main processor cabinet/chassis located in their corresponding divisional DCIS rooms in the CB.

The TCM shown in Figure 4-17 allows the TRICON to communicate with TriStation, other TRICONs, Ethernet devices, and Modbus master and slave devices. Each TCM contains four serial ports, two network ports, and one debug port (for Triconex use). Each serial port is uniquely addressed and can be configured as a Modbus master or slave. Serial port #1 supports either the Modbus or the Trimble GPS interface. Serial port #4 supports either the Modbus or the TriStation interface. Each TCM supports an aggregate data rate of 460.8 kilobits per second, for all four serial ports. For ESBWR application these ports are used only for setup of the TRICON and are normally disconnected.

Each TCM contains two network ports identified as NET 1 and NET 2. Models 4351A and 4353 have two copper Ethernet (802.3) ports and Models 4352A and 4354 have two fiber optic Ethernet ports; the fiber optic version is used by the ESBWR application. NET 1 and NET 2 support the TCP/IP, Modbus TCP/IP Slave/Master, TSAA, TriStation, SNTP, and Jet Direct (for network printing) protocols. NET 1 also supports the Peer-to-Peer and Peer-to-Peer Time Synchronization protocols.

A single TRICON system supports a maximum of four TCMs, which must reside in two logical slots; the ESBWR application uses four TCMs per division.

The TCM is a safety-related component located physically within a division in the main chassis/cabinet and controls communication access to and from the TRICON main (application) processors; there is no direct external connection to the application processors. The physical “output” of the TCM card is fiber and the portion of the TCM in which signals are first turned to light is the electrical isolator. The fibers themselves (although they cannot conduct electricity) are not credited as isolators and serve only as communications media.

Each divisional TRICON main processor cabinet contains ten safety-related small network switches arranged in pairs and used to increase communications reliability. The switches are arranged in rings and the resulting communications are self-healing. This means that if a fiber or switch is broken in one direction of the ring, data can still reach its destination in the other direction. The ESBWR application communications architecture is multiple failure proof.

Figure 4-13 Division 1 TRICON Communications

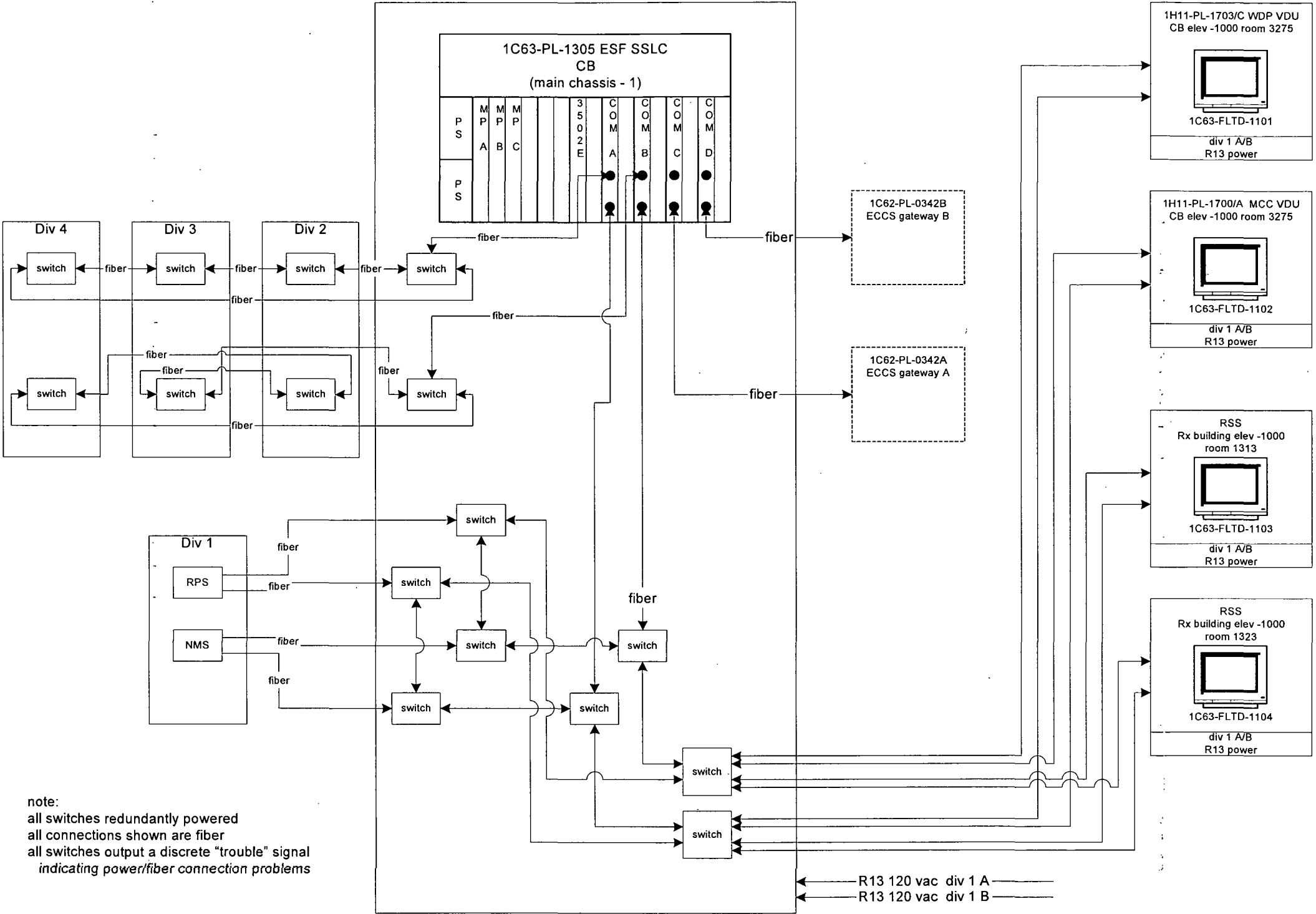


Figure 4-14 Division 2 TRICON Communications

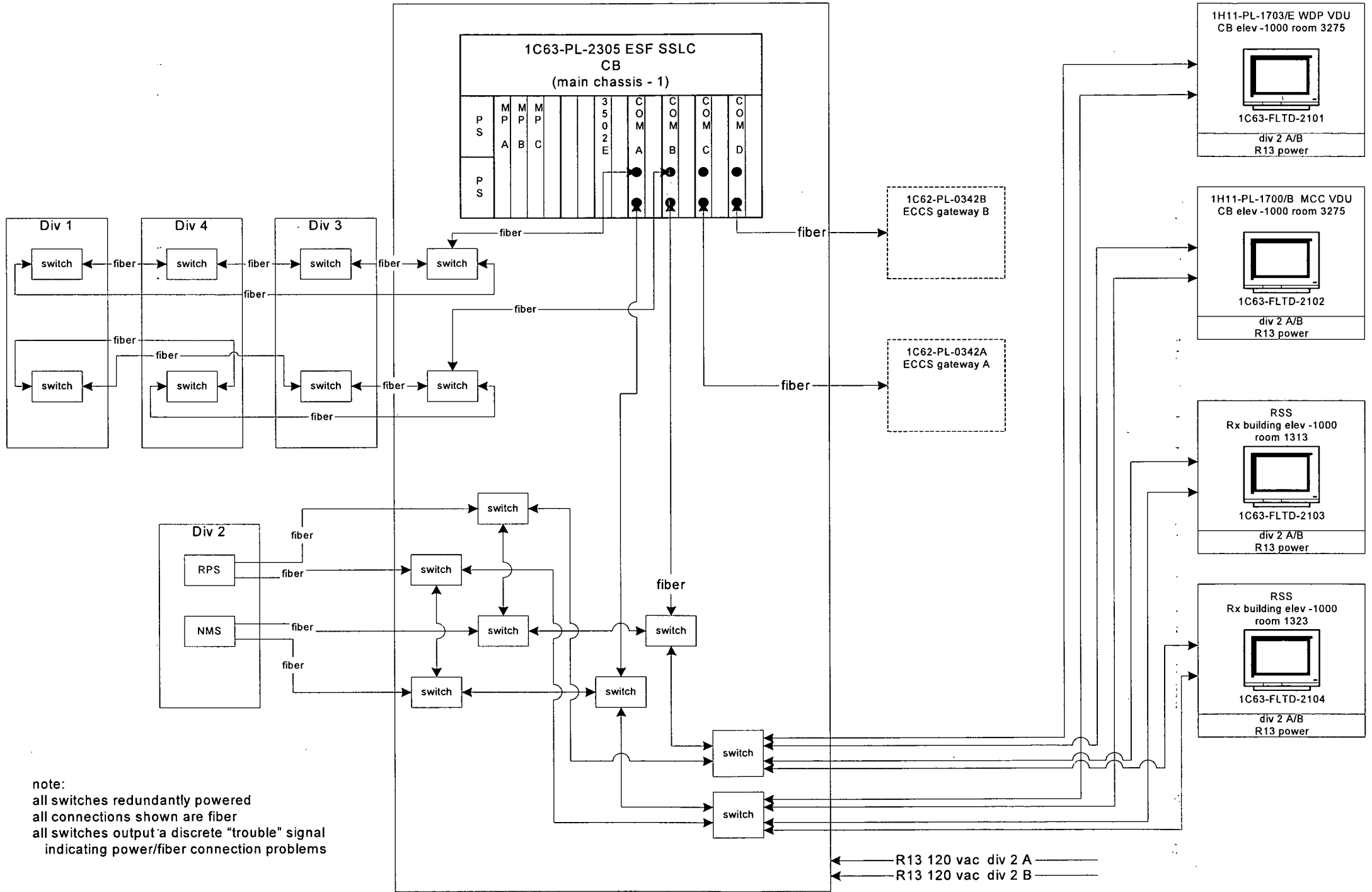


Figure 4-15 Division 3 TRICON Communications

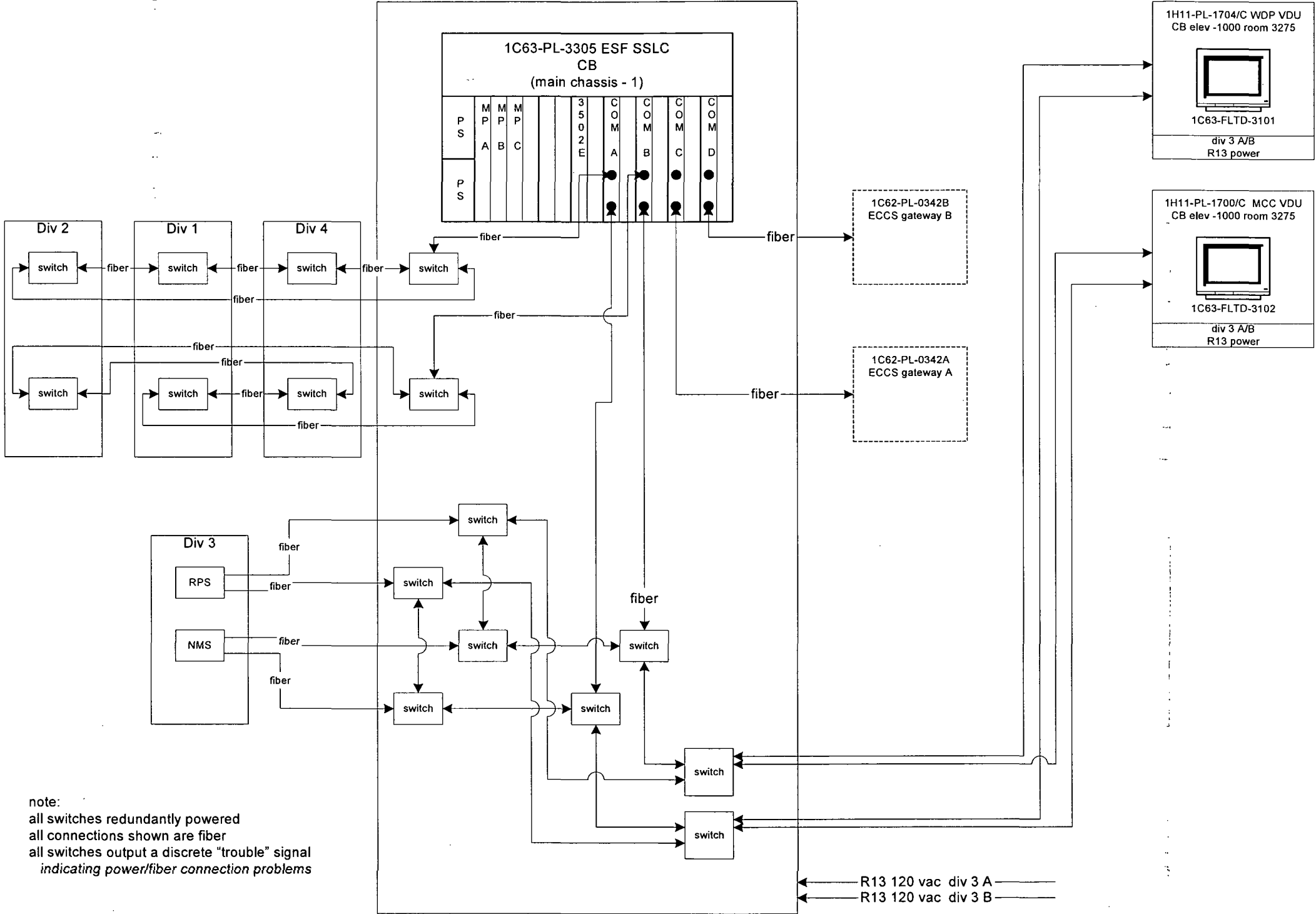
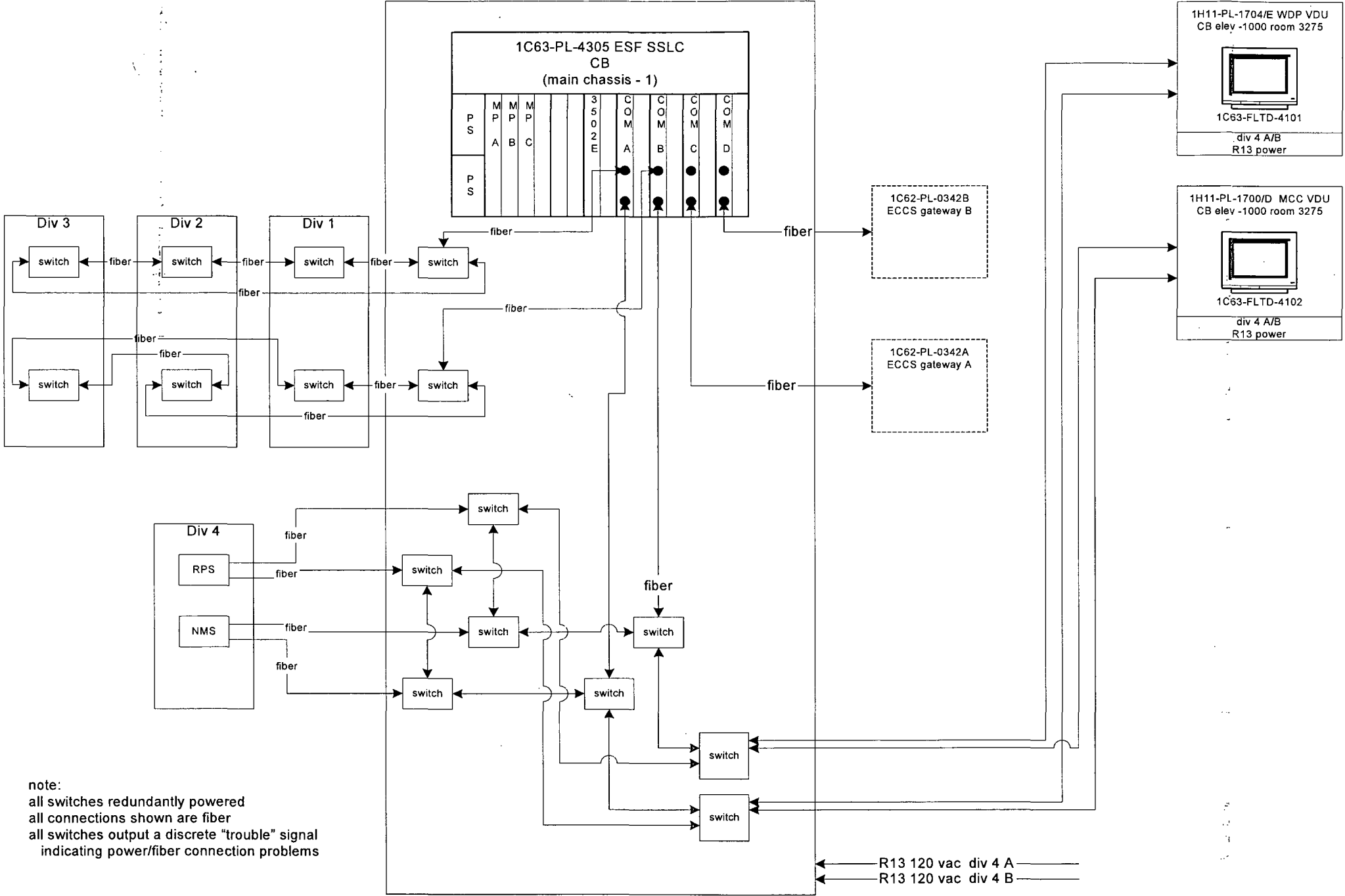


Figure 4-16 Division 4 TRICON Communications



The switches are smart enough to identify that a fiber is broken in one ring direction and, even though data are still getting through, will close a contact monitored by the TRICON to indicate that a failure has occurred. Each of the paired switches in a division is powered by different 120 VAC power feeds. There are two such self-healing rings and either supports the SSLC/ESF with no loss of system functionality.

The first communication path is used for the interdivisional communication that supports the two out of four logic used for the various ECCS initiations. This path is by fiber and redundant and, as with the other communication paths, monitored by the network switches. The redundant paths are deliberately not symmetric since the two network switches within each division that support the two paths are actively powered. The implication is that in the unlikely event of a division completely losing power, the required communications could not go “through” that division to the unfailed ones. Since the ESBWR is designed to be N-2, the redundant paths are set up as follows:

Div 1 > Div 2 > Div 3 > Div 4 > Div 1

and

Div 1 > Div 3 > Div 2 > Div 4 > Div 1

This arrangement shows that even with any two random divisional failures, the remaining two divisions can still communicate to support a two out of four initiation signal.

The second communication path is from the TRICON to the safety-related VDUs; this path combines the NUMAC links with the TRICON so that both sets of data can be displayed. Nominally the number of VDUs is two per division in the MCR with an additional pair in both divisions 1 and 2 for the RSS. The design of the network switches can accommodate more or less VDUs as final MCR and plant design dictates. The communication links also carry operator commands to the TRICON – typically for manual initiation of ECCS; since these links are within the division there is no possibility of affecting another division. A VDU is actually a combination of a safety-related display controller and safety-related display. The display controller is a separate processor from the triply redundant TRICON main processors that run the SSLC/ESF application programs.

The third communication path is from the TRICON to N-DCIS and is used to send SSLC/ESF data to the nonsafety-related alarm management, monitoring, and recording systems. The fiber from the TRICON TCM is connected to a nonsafety-related gateway where the already isolated data is translated to become compatible with the N-DCIS networks. These links have their own TCMs which have the ability to be set up as “read only” to preclude the possibility of the N-DCIS controlling or affecting operation of any safety-related function. The ESBWR application does not include control of safety-related systems from any nonsafety-related component or from any safety –related component outside of its division. Data from the TRICON is deliberately kept as simple as possible, i.e. the divisional information is “broadcast” to the gateways, which are then responsible for packaging and responding to nonsafety-related queries. Data to the TRICON is limited to time-of-day information that is deliberately not used to synchronize any safety-related function or division. No safety-related application or function is dependent on any nonsafety-related data or its accuracy nor even the existence of the fiber links or the gateways.

The fourth communication function is a redundant link from the NUMAC NMS and RPS that allows those data to be displayed on the safety-related VDUs (the NUMAC data also has isolated

links to N-DCIS to allow the same data to be displayed on nonsafety-related VDUs). Since the NUMACS are not “controlled” in normal operation (other than by dedicated MCR hard switches), the links are “one-way” for alarms, monitoring and NUMAC diagnostics. The NUMAC to TRICON links are entirely within each division.

In summary, the TRICON communications are such that:

- No functionality is lost within a division with any single fiber or network switch failure.
- No data are lost to N-DCIS with any single fiber failure.
- No overall SSLC/ESF ECCS functionality is lost with the failure of any two divisions including their network switches or fibers.

4.2.7 TRICON VDUs

The qualification details of the TRICON VDU are included in Reference 13, with both display operating and application software included; additionally the physical display and display controller are qualified to both seismic and environmental standards including a temperature requirement of 50 deg C.

The VDU is redundantly powered and each has two fiber links (communication paths) to the TRICON. Because there are no electrical or data connection to the VDU from other divisions or N-DCIS, the ESBWR application does not require safety-related to nonsafety-related isolation. Additionally each VDU within a division is independent in that it can be substituted for both control and monitoring for any other VDU within a division; a division is not out of service because of the failure of one VDU. If a VDU or network switch or communication path has failed and is subsequently returned to service, the operator does not have to perform any specific tasks; the repaired/replaced components reinitialize automatically.

Both the safety-related and non safety-related VDUs are connected to their corresponding networks by fiber and the communication scheme is designed to include recognition, verification and handshaking such that the possibility of inadvertent actuation is essentially eliminated. This means that any VDU in a given location remains viable despite the failure or destruction of other VDUs in different locations. In all cases it is the divisional TRICON’s function to determine the validity of any messages sent to it, not the VDU or other divisional TRICONS.

The VDU application software is ACCIS and it is qualified to provide at least the following VDU functions:

- Touch screen interface for menu navigation and plant control
- At least once/second screen update capability
- Trend plot capability
- Simple alarm management (when N-DCIS is unavailable)
- 19 to 24 inch widescreen (16 X 9) display format
- Storage for approximately 100 display formats (per VDU)
- Less than one second response to operator demands
- Self-diagnostics
- Capability to have the same operator “look and feel” as the nonsafety-related VDUs
- A scheme requiring two or more operator actions before any control action is initiated

Although not used in normal TRICON operation, the software used to construct display formats for the VDUs is also being qualified.

4.2.8 TRICON Security

Many of these security features are discussed in the TRICON safety evaluation report (Reference 14, but because they are used in the ESBWR SSLC/ESF application, they are discussed in this report.

4.2.8.1 Physical Security

All of the TRICON chassis are installed in locked cabinets that include a cabinet door position switch that is monitored by the N-DCIS (so that it will be monitored even if the TRICON is disabled).

Additionally the TRICON main cabinet (which is the only cabinet that has the SSLC/ESF application software) includes a main chassis keylock switch. This is a four-position switch that controls all the chassis in the division and is readable by the TRICON, the application software and Tristation software used to program the TRICON. (The Tristation software is used to implement the SSLC/ESF application logic developed by the various system engineers and enforces compatibility with the TRICON; then the Tristation can be connected to the TRICON and the application software downloaded with the keylock switch in the “program” position. After a successful download the Tristation is disconnected, the keylock switch is positioned in “run” or “remote,” and the key is removed, making it impossible to change the application software.)

Switch settings are:

- RUN – This represents the normal operation of the TRICON where the main processors execute the previously loaded application program. The key is normally removed from the TRICON and kept under plant administrative control. Any attempts to modify program variables by TriStation, Modbus masters or external hosts are rejected.
- PROGRAM - This switch position is used for program loading and checkout. It allows control of the TRICON system from the TriStation platform, including the downloading of new application software.
- STOP – In this position the TRICON stops reading inputs, forces non-retentive digital and analog outputs to zero, and halts the application software. (Retentive outputs retain the value they had before the keylock switch was turned to STOP.) The STOP setting can be used for installation and service of process related equipment, but is not required for service of the TRICON. Additionally the STOP position may be application software disabled to prevent inadvertent shutdown of the TRICON.
- REMOTE – In this position the TRICON allows updates to program variables by TriStation and external hosts. Modification of the application software is not allowed.

4.2.8.2 Communications Security

Q-DCIS communications:

- Never corrupt another division
- Never depend on any nonsafety-related communication or data
- Never allow nonsafety-related communication or data to corrupt safety-related functions

The TRICON communications design is governed by Reference 7 requirements for data isolation and independence.

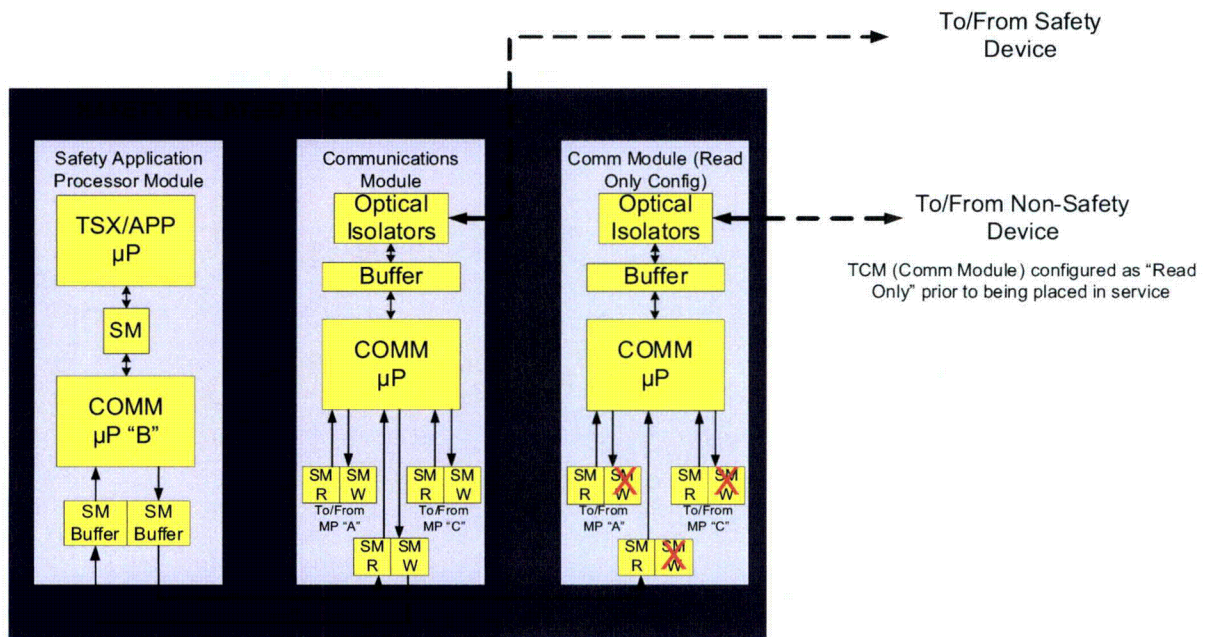
4.2.8.2.1 *Hardware Security*

As shown in Figure 4-17, the triply redundant main processor modules have separate application and communication processors and only communicate through shared memory; this is the first of the “double buffers”. The main processor communication processor is only connected to the separate communication module card with its own processors through shared memory; this is the second of the “double buffers”. All of these processors and communications are asynchronous.

Within the TRICON all data writes must be in the proper format, have the proper address, and be within a given range. The application programmer must pre-designate points as writeable with the application software, otherwise no writes are allowed whatever an outside device sends. Additionally these pre-designated points must be programmed into the sending TRICON.

As a result of the buffering, the triply redundant safety-related application processors never handle “read” (i.e. from the TRICON) requests. Instead for every program scan there is a full data dump to the communication module of all user predefined (programmed) readable points and all diagnostics values.

Figure 4-17 TRICON Communications Module



The TRICON external communications schemes use a "Black Channel" definition illustrated in Figure 4-18 meaning that everything outside of the TRICON is considered unknown. All design criteria and functions needed to meet the required divisional independence and isolation and to maintain data integrity are contained within the safety-related TRICON, specifically the communications module, the MP application processors and the MP communications processors. With this concept it is irrelevant whether or not the communication paths are point to point or networked since it does not matter how the data gets to the TRICON. No credit is taken for external devices whether they are nonsafety-related or a TRICON in another division. Full electrical isolation is provided by optical isolators within the division and the required use of fiber between divisions and between Q-DCIS and N-DCIS.

The TRICON system maintains multiple barriers between the main processors performing the application software and the communication process to external devices. These include:

- Shared Memory
- Buffers

- Two barrier processors between the safety-related application processor and the “outside” world
- Capability to disable write functions per communications card
- “Read” methodology that ensures no requests go further than the communication card
- Isolation / data independence from external devices and controlled fully within the TRICON system

Figure 4-18 TRICON Communications Security

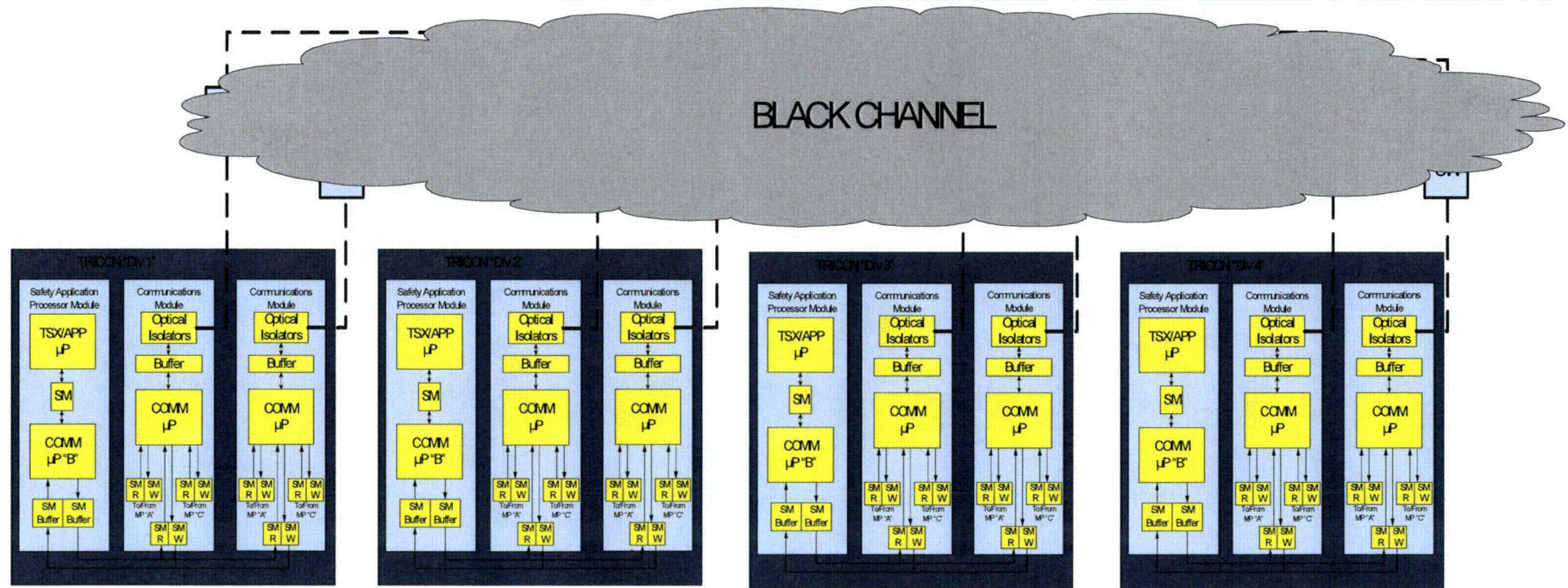


Figure 4-17 also indicates that there are several communication modules per division; the TCMs that handle safety-related to safety-related communication are separate from those handling Q-DCIS to N-DCIS communication. The latter TCMs are configured as “Read Only,” with all write functions to the TRICON disabled; and all write requests are ignored.

At the end of every triply redundant main safety-related application processor scan, all data pre-defined as “Read” or “Read-Write” and all diagnostics are dumped all the way to the TCM card memory. Then the sequence for the TCM is:

- A request for data comes into the TCM
- The TCM looks only to its own memory (not the application processor) for available data on a read request
- Acceptable read requests can only be for the listed read points or the request is ignored
- Only then are data transmitted out to service the read request

Because there are separate TCMs for safety-related to safety-related communications and Q-DCIS to N-DCIS communications, it is possible to make available only the data needed for two out of four logic to the former TCMs while essentially all divisional data can be made available to the read only Q-DCIS to N-DCIS communications.

Communications to and from the TRICON VDUs accommodate the fact that operator inputs cannot be anticipated but must nevertheless be secure. Figure 4-19 illustrates the sequence.

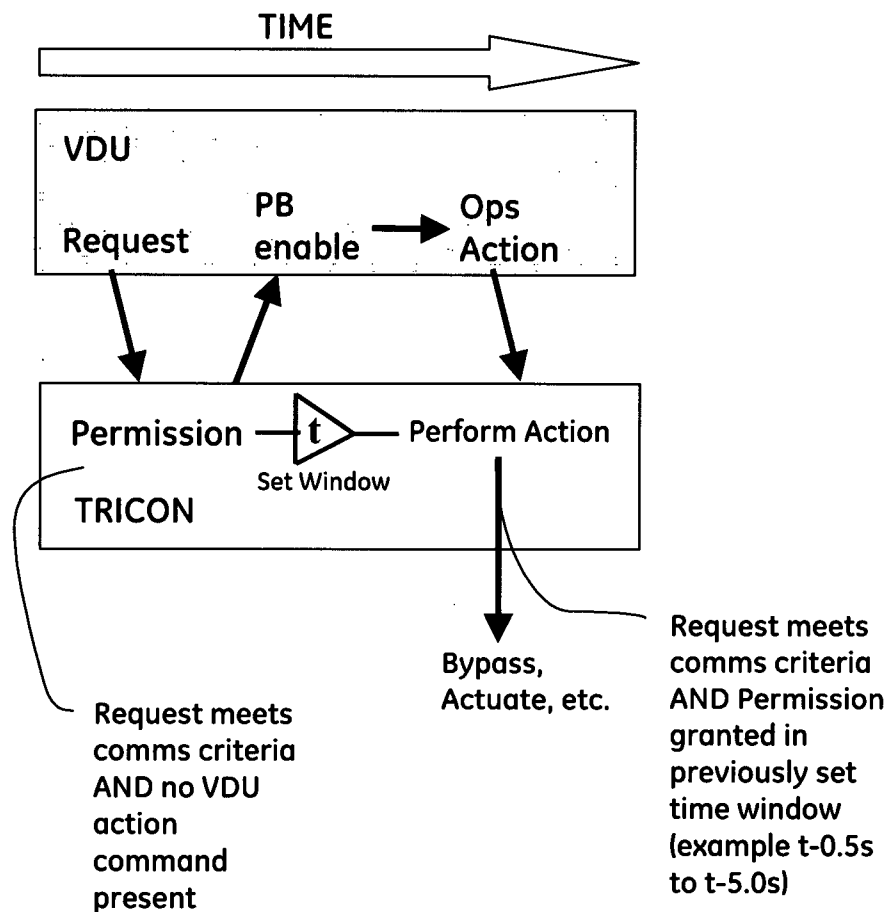
For any operator input (typically a touchscreen action), the VDU requests permission from the TRICON. If the TRICON recognizes the VDU as a legitimate communication link, it simultaneously grants permission to the VDU, and starts an internal TRICON timer. The operator touchscreen demand must still exist within the timer’s “window”; otherwise the action is refused. This sequence occurs for each of the at least two VDU actions (i.e. “select” then “actuate”) that the operator must perform for any manual action.

The above timing and authentication scheme essentially makes any VDU operating or application software failure affecting the TRICON application software incredible. The scheme also makes incredible the potential for VDU failures causing inadvertent actuations.

4.2.8.2.2 *Message Authentication*

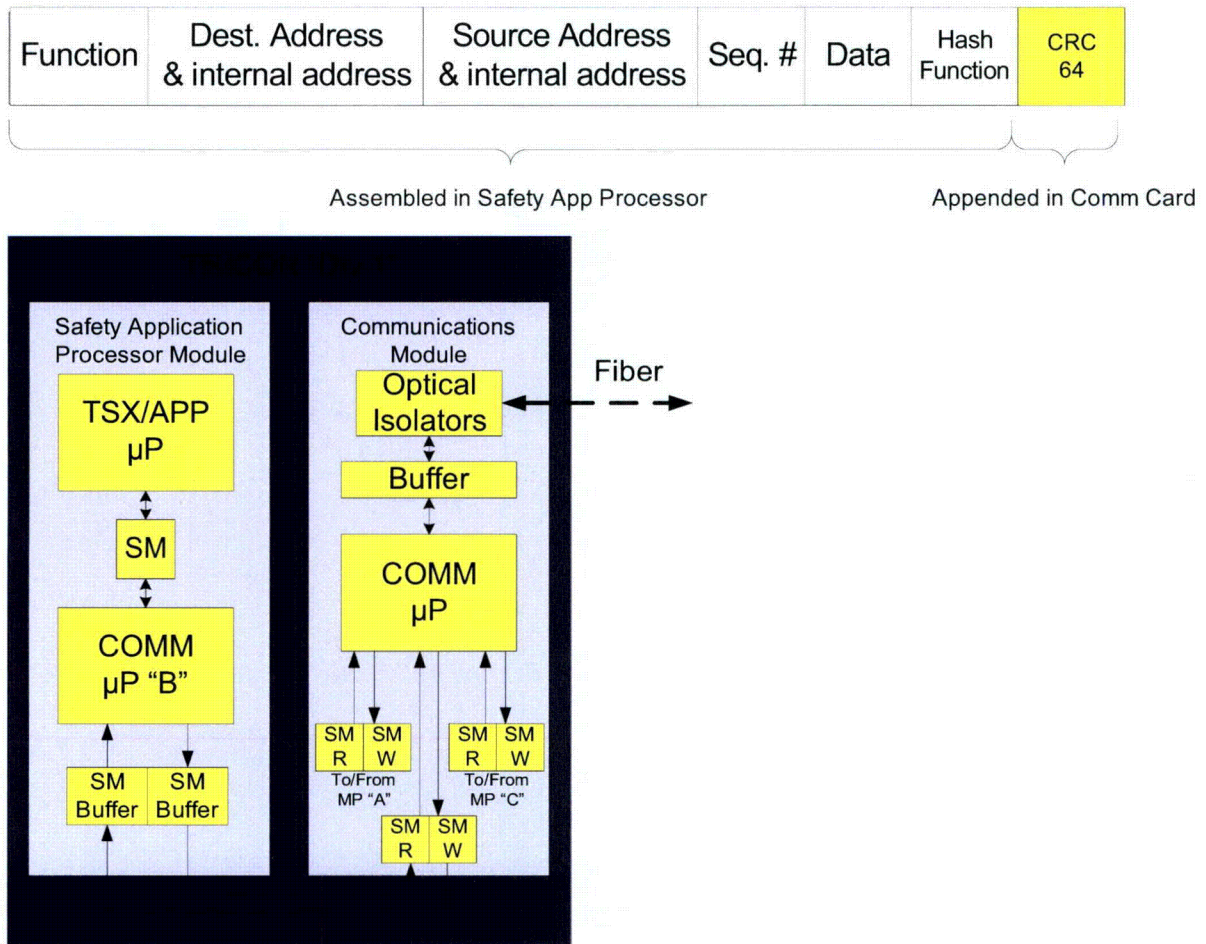
The TRICON hardware provides control of physical or inappropriate access to the TRICON application software but it is also important to ensure the authenticity and reliability of the messages being transmitted between the various safety-related devices, both to ensure that a message from an appropriate device should be accepted and to ensure that the message content has not been corrupted.

Figure 4-19 TRICON/VDU Communications



Message authentication uses several schemes, the TRICON to TRICON Peer-to-Peer (used for the two out of four ECCS initiation logic) is a proprietary protocol that is essentially a point to point User Datagram Protocol (UDP) / Internet Protocol (IP) non-request transmission with an additional safety communication layer on top of the standard communication layers. The TRICON expects a feedback message for every transmission. If the message is lost (non-validated), the sending unit will take action (alarm) and the receiving unit will take action (fail-as-is or fail-safe as appropriate) as defined in the application software. The user can define specific actions to be taken on loss of validated data/communication in the application program.

Additional techniques for message authentication are illustrated in the example of the TRICON communication message structure in Figure 4-20.

Figure 4-20 TRICON Message Structure

Addresses, internal addresses, data formats and ranges, and data point IDs are all preprogrammed in each TRICON system. Messages that are in an improper format are rejected.

Connection authentication is enforced by having messages include a unique source and destination identifier that describes the logical address of the safety-related participant. (These are also included in the feedback message).

A sequence number is integrated into messages exchanged between message source and message receiver. It is implemented as an additional data field with a number that changes from one message to the next in a predetermined way. Non-responsiveness causes the TRICONs to reset sequence numbers. Sequence numbers are not skipped.

The safety-related application process does not assume that the incoming data transmission integrity is assured by the sender, instead redundant data is included in the message to permit data corruptions to be detected by methods used by the receiver of the data. These include a hash function that takes a message of variable length as input and produces a fixed-length string as output, referred to as hash-code or simply hash of the input message. More specifically a hash function is used to create a digital signature that can identify and authenticate both the sender and message of a digitally distributed message. Additionally included are several cyclic redundancy checks, a technique used for detecting data errors occurring during transmission. Transmitted messages are divided by the sending processor into predetermined lengths that are then divided by a fixed denominator. The remainder result of that division is appended onto and sent with the message. When the message is received, the receiving processor recalculates the remainder and compares it with the transmitted remainder. If the remainders do not match, an error is indicated.

The end result of these techniques is that it is essentially impossible for the TRICON application software to be affected by an external source, independent of how often those sources may make the attempt. It is equally unlikely that a message sent from one TRICON (division) to another can be incorrectly interpreted or that the sending TRICON can affect the receiving TRICON's application software. It is also highly unlikely that any division can accept operator demands from any other division or from N-DCIS or that any division or VDU could generate inadvertent commands or initiations.

[[

]]

5.0 NRC CERTIFICATION – GE RESPONSE TO OPEN ITEMS

The NRC has approved the Triconex Topical Report 7286-545-1-A, "Qualification Summary Report " (Reference 14). Although this topical report was approved by NRC, the staff safety evaluation defines the basis for acceptance of the report in the SER section 5.2 with 18 items identified as plant-specific requirements.

5.1 Item #1: Qualification for Temperature and Humidity Conditions.

“Section 4.1.3.2 of this SE discusses the temperature and humidity conditions for which the TRICON PLC system is qualified. Licensees will be responsible for analysis of the plant-specific environment, and the determination that the TRICON PLC system is suitable for that particular plant usage.”

DCD Tier 1, Rev. 3, Item 1 of Table 2.2.13-1, “ITAAC for safety system logic and control (SSLC/ESF) system” addresses the basic configuration of the system. Section 1.2.2.1 of DCD Tier 1 defines the verifications for the basic configuration of the system as including temperature and humidity conditions [Subparagraph (3)]. DCD Tier 2, subsection 7.1.6.6.1.5 addresses the temperature and humidity conditions for qualification of Q-DCIS components.

5.2 Item #2: Qualification for Radiation Exposure Levels.

“Section 4.1.3.3 of this SE discusses the radiation exposure levels for which the TRICON PLC system is qualified. Licensees will be responsible for analysis of the plant-specific radiation environment, and the determination that the TRICON PLC system is suitable for that particular plant usage.”

DCD Tier 1, Rev. 3, Item 1 of Table 2.2.13-1, “ITAAC for safety system logic and control (SSLC/ESF) system” addresses the basic configuration of the system. Section 1.2.2.1 of DCD Tier 1 defines the verifications for the basic configuration of the system as including radiation effects [Subparagraph (3)]. DCD Tier 2, subsection 7.1.6.6.1.5 addresses the radiation conditions for qualification of Q-DCIS components. MFN 07-458 Enclosure 1 Page 3 of 8 [Subparagraph (3)].

5.3 Item #3: Qualification for Seismic levels.

“Section 4.1.3.4 of this SE discusses the seismic levels for which the TRICON PLC system is qualified. The staff found that the TRICON PLC system did not fully meet the guidance of EPRI TR-107330 for seismic requirements, and before using TRICON PLC system equipment in safety-related systems in a nuclear power plant, licensees must determine that the plant-specific seismic requirements are enveloped by the capabilities of the TRICON PLC system”.

DCD Tier 1, Rev. 3, Item 1 of Table 2.2.13-1, “ITAAC for safety system logic and control (SSLC/ESF) system” addresses the basic configuration of the system. Section 1.2.2.1 of DCD Tier 1 defines the verifications for the basic configuration of the system as including design basis dynamic loads [Subparagraph (2)]. DCD Tier 2, subsection 7.1.6.6.1.5 addresses the seismic qualification of Q-DCIS components.

5.4 Item #4: Qualification for EMI/RFI: Conducted or Radiated Emissions.

“Section 4.1.3.5 of this SE discusses the conducted or radiated EMI/RFI emissions or susceptibility for which the TRICON PLC system is qualified. Since the TRICON PLC system did not satisfy the guidance of EPRI TR-102323, it is the responsibility of the licensees to measure or otherwise determine the worst case EMI/RFI environment that would exist at the time the protective function provided by the TRICON PLC system would be required, and then to ensure that the conducted and radiated EMI/RFI emissions and susceptibility capabilities of the TRICON PLC system envelop this environment, and that the system will not affect surrounding equipment.”

DCD Tier 2, subsection 7.1.6.6.1.5 addresses the EMC compatibility of Q-DCIS components. DCD Tier 2, subsection 7.1.3.2 addresses the EMI/RFI and EFT (surge) qualification of Q-DCIS components. DCD Tier 2, subsection 7.1.6.4 lists and discusses the specific regulatory requirements for EMI/RFI, and EFT qualification of Q-DCIS components. These design requirements are applied to the procurement of safety-related components in accordance with the GE Quality Assurance Plan (see DCD Chapter 17). A separate ITAAC to demonstrate design conformance with EMI/RFI is not proposed based on the assurance of the established design controls.

5.5 Item #5: Surge withstand capability.

“Section 4.1.3.6 of this SE discusses the surge withstand capabilities for which the TRICON PLC system is qualified. Licensees will be responsible for the analysis of the plant-specific surge environment, and the determination that the TRICON PLC system is suitable for that particular plant usage.”

DCD Tier 2, subsection 7.1.3.2 addresses the EMI/RFI and EFT (surge) qualification of Q-DCIS components. DCD Tier 2, subsection 7.1.6.4 lists and discusses the specific regulatory requirements for EMI/RFI, and EFT qualification of Q-DCIS components. These design requirements are applied to the procurement of safety-related components in accordance with the GE Quality Assurance Plan (see DCD Chapter 17). A separate ITAAC to demonstrate design conformance with EMI/RFI is not proposed based on the assurance of the established design controls. MFN 07-458 Enclosure 1 Page 4 of 8.

5.6 Item #6: Electrostatic Discharge (ESD) Withstand Capability.

“Section 4.1.3.7 of this SE discusses the ESD withstand capability, and the fact that the TRICON PLD system was not tested for this capability. Before installing and using the TRICON PLC system, licensees must have in place administrative or physical controls to ensure that no activity which would require opening the cabinet can take place while the TRICON PLC system is required to provide its protective function, unless the particular cabinet and all channels within that cabinet are placed in a trip or bypassed condition according to plant procedures. An alternative solution is for licensees to perform sufficient testing and analysis to demonstrate that the ESD withstand capability of the TRICON PLC system envelops the plant-specific requirements.”

DCD Tier 2, Subsection 7.3.5.5, addressing the ESD withstand capability will be revised as shown.. This revision to the DCD is consistent with Triconex discussions of the ESD withstand capability of the Tricon PLC System with the NRC staff from a meeting dated 11/18/2004

(accession number ML043380096). With the imposition of these requirements, a separate ITAAC to demonstrate ESD withstand capability is not proposed.

5.7 Item #7: Safety-Related to Nonsafety-related Isolation from Credible Voltages.

“Section 4.1.3.8 of this SE discusses the Class 1E to non-1E isolation capabilities for which the TRICON PLC system is qualified. Licensees will be responsible for analysis of the plant-specific maximum credible applied voltages produced by non-1E interfaces, and for ensuring that this value is enveloped by the TRICON PLC system capacity, and that the TRICON PLC system is suitable for that particular plant usage.”

MFN 07-402 provides DCD Tier 1 changes to reflect ITAAC for design conformance to IEEE Std. 603 in Table 2.2.15-2. ITAAC for Criterion 5.6, Independence addresses the design of the safety to non-safety isolation.

5.8 Item #8: Software Installation Plan Development.

“Section 4.2.2.5 of this SE discusses the software installation plan. The staff determined that the software installation plan is the responsibility of the licensee, and must be developed before the TRICON PLC system software can be used for safety-related applications in nuclear power plants.”

The IPS software quality development plan complies with the Standard Review Plan, Branch Technical Position (BTP) 14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”. The SIP is presented in NEDE-33226, “ESBWR I&C Software Management Plan,” (SMP) submitted by MFN-07-384, dated July 24, 2007. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Item 5. MFN 07-458 Enclosure 1 Page 5 of 8.

5.9 Item #9: Software Maintenance Plan Development.

“Section 4.2.2.6 of this SE discusses the software maintenance plan. Although Triconex has an acceptable software maintenance plan, the staff determined that a plant-specific software maintenance plan is also required, and it is the responsibility of licensees to develop this software maintenance plan before the TRICON PLC system software can be used for safety-related applications in nuclear power plants.”

Refer to ESBWR I&C SMP, NEDE –33226P issued to the NRC by MFN-07-384, dated July 24, 2007. The Software Operation and Maintenance Plan (SOMP) described in the SMP defines the software process and activities used to operate and maintain the software product during plant operation. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Items 1 and 6.

5.10 Item #10: Software Operations Plan Development.

“Section 4.2.2.8 of this SE discusses the software operations plan. The staff determined that licensees will be required to develop a software operations plan before using the TRICON PLC system software for safety-related use in nuclear power plants.”

Refer to ESBWR I&C SMP, NEDE –33226P issued to the NRC by MFN-07-384, dated July 24, 2007. The Software Operation and Maintenance Plan (SOMP) described in the SMP defines the software process and activities used to operate and maintain the software product during plant operation. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Item 6.

5.11 Item #11: Software Safety Plan Development.

“Section 4.2.2.9 of this SE discusses the software safety plan. The staff determined that licensees will be required to develop a software safety plan before using the TRICON PLC system software for safety-related applications in nuclear power plants.”

Refer to ESBWR I&C Software Quality Assurance Plan (SQAP) NEDE –33245P issued to the NRC by MFN-07-384, dated July 24, 2007. The SQAP contains the Software Safety Plan (SSP) description. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Item 8.

5.12 Item #12: Software Verification and Validation.

“Section 4.2.2.10 of this SE discusses verification and validation. Although Triconex did not strictly follow guidelines of IEEE Std 1012, the staff determined that the combination of the internal Triconex review, the TÜV certification, and the review by MPR and ProDesCon provided acceptable verification and validation for software that is intended for safety-related use in nuclear power plants. However, the staff noted that a significant portion of its acceptance is predicated upon the independent review by TÜV-Rheinland, and licensees using any TRICON PLC system beyond Version 9.5.3 must ensure that similar or equivalent independent V&V is performed; without this, the TRICON PLC system will not be considered acceptable for safety-related use at nuclear power plants. Should licensees use future TRICON PLC systems beyond Version 9.5.3 which have not received TÜV-Rheinland certification, the staff will review the acceptability of the independent V&V during the plant-specific safety evaluation.”

MFN 07-458 Enclosure 1 Page 6 of 8 Refer to ESBWR I&C Software Quality Assurance Plan (SQAP) NEDE –33245P issued to the NRC by MFN-07-384, dated July 24, 2007. The SQAP contains the software verification and validation plan description. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Item 9..

5.13 Item #13: Impact of Tristation 1131 Use of TRICON PLC Operability.

“Section 4.2.3 of this SE discusses the use of the TriStation 1131. Section 4.2.3 of this SE noted that the Triconex PLC system is designed such that the TRICON PLC system should not be connected to a TriStation PC during safety-related operation. The plant-specific procedures which ensure that the TriStation PC is not connected to the TRICON PLC system during safety-related operation will be reviewed by the staff during the plant-specific safety evaluation. In addition, the testing of the operational software produced by the TriStation 1131, and these test plans, procedures, and results will be reviewed by the staff during the plant-specific safety evaluation.”

While the TRICON is performing safety-related functions, it will not be connected to the TriStation 1131 PC during normal operation. Refer to NEDE –33226P, "ESBWR I&C Software Management Plan," (SMP) issued to the NRC by MFN-07-384, dated July 24, 2007. The SOMP described in the SMP defines the process and activities used to operate and maintain the software product during plant operation. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Item 6.

5.14 Item #14: Plant Specific Application Program.

“Section 4.2.4 of this SE discusses the application programs, which are inherently plant specific, and therefore are not included in the scope of this SE.”

The Invensys software quality development plan complies with the Standard Review Plan, Branch Technical Position (BTP) 14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems". The application software programmed for the SSLC/ESF and the associated test plans, procedures, and results will be governed by NEDE-33245P, "ESBWR - I&C Software Quality Assurance Plan (SQAP)." For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2-1, Item 3.

5.15 Item #15: Component Aging Analysis.

"Section 4.3.3 of this SE discusses the component aging analysis, which determined that the chassis power supplies and backup batteries are susceptible to significant, undetected aging mechanisms. Before installing TRICON PLC system equipment in a nuclear power plant, licensees must have procedures in place to ensure periodic replacement of these components."

Aging degradation of these components can be effectively addressed through periodic replacement prior to onset of significant loss of performance. Periodic preventive maintenance is an activity performed at regular intervals to preclude problems that could occur before the next preventive maintenance (PM) interval as discussed in subsection 17.4.9 of DCD, Tier 2, 26A6642BW, Rev. 3. For ITAAC, refer to Tier 1, Rev. 3, Table 3.6-1. MFN 07-458 Enclosure 1 Page 7 of 8.

5.16 Item #16: Response time Characteristics.

"Section 4.3.5 of this SE discusses the response time characteristics of the TRICON PLC system software safety plan. The staff determined that the actual response time for any particular system will depend upon the actual system configuration, and may vary significantly from simple to complex systems. The determination of the response time for the particular system intended for safety-related use for a particular plant application, and the determination that this response time satisfies the plant specific requirements in the accident analysis in Chapter 15 of the safety analysis report is the responsibility of the licensee."

The SSLC/ESF platform operating the ESBWR specific application will be tested during factory acceptance testing. The testing will specifically confirm required response times. There is no credible failure mode that can change the system response time. In addition, a DCIS or specific ECCS system preoperational test will be conducted to verify the ability to transmit and receive data from interfacing systems within specified response times and data rate requirements (see subsection 14.2.8.1.7). Also refer to the ESBWR SMP that contains a hardware/software specification description of the algorithms and functions too complex to be delineated in the logic diagrams, including response time requirements. For ITAAC, refer to DCD Tier 1, Rev. 3, Table 3.2 1, Items 1 and 6.

5.17 Item #17: Diversity and Defense-in depth (D3).

"Section 4.3.10 of this SE discusses diversity and defense-in-depth. A review of the differences between the TRICON PLC system and the non-safety control system implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in-depth continue to be maintained must be addressed in a plant-specific D-in-D&D evaluation".

This has been addressed by Licensing Topical Report NEDO 33251, "ESBWR I&C Defense-In-Depth and Diversity report", Revision 1, (submitted August 31, 2007, as stated in MFN-07-265

dated June 1, 2007). The NEDO- 33251 Revision 1 update will include vendor specific information for the SSLC/ESF platform. For ITAAC, refer to Tier 1, Rev. 3, Table 2.2.14-1.

5.18 Item #18: Qualification Summary Report “Applications Guide” Recommendations.

“Triconex has made a number of determinations of items and criteria to be considered when applying the TRICON PLC system to a specific plant application. These are contained in the "Applications Guide," provided as Appendix B to the "Qualification Summary Report," Triconex document number 7286-545. A number of these are the same as those discussed above, but the "Applications Guide" goes beyond regulatory compliance to include good engineering practice and applications suitability determinations. It is expected that licensees intending to use the TRICON PLC system will consider each item in this guide, and document the appropriate decisions and required analysis”.

This LTR addresses the specific ESBWR application of the TRICON for use as the SSLC/ESF hardware/software platform. All of the Triconex Application Guide recommendations have been or, in detailed design, will be addressed and documented.

6.0 REFERENCES

1. 26A6641AB (Tier 1, Rev. 3, February, 2007), 26A6642AW (Tier 2 Rev. 3, February 2007), "ESBWR Design Control Document"
2. NEDE-33245P LTR "ESBWR Software Quality Assurance Plan, revision 2" July 2007
3. NEDE-33226P, LTR "ESBWR I&C Software Management Plan, revision 2", July 2007
4. NEDO-33201, "ESBWR Certification Probabilistic Risk Assessment" (not yet issued)
5. NUREG- 0493, "A Defense-in-Depth & Diversity Assessment of the RESAR – 414 Integrated Protection System," March 1979
6. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, " December 1994
7. IEEE 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
8. IEEE 379-2000, "IEEE Standard Application of the Single-failure Criterion to Nuclear Power Generating Station Safety Systems – Description"
9. R.G. 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," May 1973
10. General Design Criterion 24, Separation of Protection and Control Systems
11. RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident"
12. NEDO-33251 LTR "ESBWR I&C Diversity and Defense-in-Depth Report," Rev. 1, August 2007
13. Triconex Report 7286-547, "Safety-related Video Display Unit (VDU) Programmatic Topical Report," Rev. 0 (to be issued)
14. NRC Safety Evaluation Report (SER) ML013470433, Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 To Qualification Summary Report," Revision 1

MFN 07-515

Enclosure 3

Affidavit

GE-Hitachi Nuclear Energy, LLC

AFFIDAVIT

I, David H. Hinds, state as follows:

- (1) I am the General Manager, New Units Engineering, GE-Hitachi Nuclear Energy Americas LLC (GEH) have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.
- (2) The information sought to be withheld is contained in Enclosure 1 of GEH letter MFN 07-515, Mr. James C. Kinsey to U.S. Nuclear Regulatory Commission, entitled *Licensing Topical Report NEDE-33388P, Revision 0, ESBWR I&C TRICON (SSLC/ESF) Platform Application*. The proprietary information in Enclosure 1, which is entitled *GEH Nuclear Energy, "ESBWR I&C TRICON (SSLC/ESF) Platform Application," NEDE-33388P, September 2007 – Proprietary Version* is delineated by a [[dotted underline inside double square brackets^{3}]]. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation ^{3} refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.
- (3) In making this application for withholding of proprietary information of which it is the owner, GEH relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.790(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).
- (4) Some examples of categories of information which fit into the definition of proprietary information are:
 - a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by GEH competitors without license from GEH constitutes a competitive economic advantage over other companies;
 - b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

- c. Information which reveals aspects of past, present, or future GEH customer-funded development plans and programs, resulting in potential products to GEH;
- d. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a, and (4)b, above.

- (5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GEH, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GEH, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements, which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.
- (6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge. Access to such documents within GEH is limited on a "need to know" basis.
- (7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GEH are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.
- (8) The information identified in paragraph (2), above, is classified as proprietary because it identifies detailed GEH ESBWR methods, techniques, information, procedures, and assumptions related to the application of the TRICON control system to the SSLC/ESF.

The development of the evaluation process along with the interpretation and application of the regulatory guidance is derived from the extensive experience database that constitutes a major GEH asset.

- (9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GEH's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GEH's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GEH.

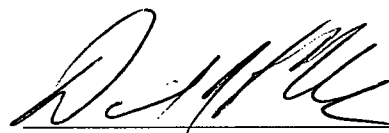
The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GEH's competitive advantage will be lost if its competitors are able to use the results of the GEH experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GEH would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GEH of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 28th day of September 2007.



David H. Hinds
GE-Hitachi Nuclear Energy Americas LLC

MFN 07-515

Enclosure 4

**DCD Tier 2 Changes to
Reflect NEDE-33388P, Revision 0**

7.3.7 References

- 7.3-5 GE-Hitachi Nuclear Energy, "ESBWR I&C TRICON (SSLC/ESF) Platform Application," NEDE-33388P, Class III (Proprietary); and "ESBWR I&CTRICON (SSLC/ESF) Platform Application," NEDO-33388, Class I (Non-proprietary) September 2007.